ESCOLA SUPERIOR ABERTA DO BRASIL – ESAB
CURSO DE PÓS-GRADUAÇÃO LATO SENSU EM
REDES DE COMPUTADORES

DANIEL LAVIERI

AS VANTAGENS DO USO DE SWITCHES DE CAMADA 3 EM REDES LOCAIS:
Como otimizar o tráfego de dados em uma rede corporativa com o uso de switches de camada 3

VILA VELHA (ES)

2013

DANIEL LAVIERI

AS VANTAGENS DO USO DE SWITCHES DE CAMADA 3 EM REDES LOCAIS:
Como otimizar o tráfego de dados em uma rede corporativa com o uso de switches de camada 3

Monografia apresentada ao Curso de Pós-Graduação em Redes de Computadores da Escola Superior Aberta do Brasil como requisito para obtenção do título de Especialista em Redes de Computadores, sob orientação do Prof. MSc. Hudson Ramos

VILA VELHA (ES)

2013

DANIEL LAVIERI

As vantagens do uso de switches de camada 3 em redes locais: como otimizar o tráfego de dados em uma rede corporativa com o uso de switches de camada 3

Monografia Aprovada em_____de _____de 2013

Banca Examinadora

_____

_____

_____

VILA VELHA - ES

2013

RESUMO

A presente monografia tem como objetivo apresentar as vantagens da utilização dos equipamentos chamados *switches* de camada 3 em redes locais de computadores corporativas. A metodologia aqui utilizada é uma pesquisa bibliográfica qualitativa de múltiplas fontes, usando-se uma abordagem do nível mais baixo para níveis mais altos. Tal abordagem consiste em apresentar conceitos fundamentais sobre topologia de redes locais, o modelo internacional para padronização de interconexão de sistemas (OSI) e uma explicação mais aprofundada de cada uma das camadas de tal modelo. A seguir serão apresentadas definições de equipamentos tais quais switches e roteadores, suas principais funções e diferenças. Também são apresentadas as definições e funcionamento de protocolos como VLAN e Spanning Tree Protocol, que servem de base para a explicação de que maneira um switch pode oferecer vantagens ao serem instalados em uma rede LAN corporativa. Como resultado obteve-se vantagens como a melhoria do tráfego de dados entre os diferentes segmentos de rede das corporações e a possibilidade de análise das melhores rotas para o encaminhamento do tráfego, além de oferecer um acréscimo global em termos de velocidade.

Palavras-chave: Redes de computadores. Comutadores de rede. Redes de computadores hierárquicas.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho aborda a temática da otimização do tráfego de dados em redes corporativas, que se insere na linha de pesquisa de Redes de Computadores. O problema central é determinar, expor e analisar quais os entraves e suas origens, e de que modo tais gargalos limitam o fluxo de dados encontrados nas redes atuais.

A importância e justificativa do tema proposto estão na necessidade de se ampliar e otimizar a oferta de banda e acrescentar melhorias na disponibilidade da rede (entendida aqui como o tempo de operação sem interrupções), para isso utilizando uma solução que engloba uma topologia de rede mais eficiente e, adicionalmente, o uso de um equipamento comutador (*switch*) que confere à rede um encaminhamento de dados inteligente entre as estações de trabalho e que atua diretamente na diminuição dos gargalos de tráfego.

As redes locais atualmente são elementos estratégicos indispensáveis a qualquer corporação. O progresso com que novas tecnologias vêm surgindo reforça essa necessidade de conectar os negócios e as atividades empresariais ao mundo da Internet, que cada vez mais se confunde com o mundo real. Dessa maneira, as redes corporativas têm sido vasto campo de estudo para a criação e o desenvolvimento de novas tecnologias. Tais avanços visam suprir as demandas de crescimento dos negócios e as necessidades de mais velocidade tanto nas transações comerciais, quanto a necessidade de armazenamento de dados e a sua transferência, bem como nas comunicações empresariais. Tais demandas trazem consigo um crescimento das redes corporativas e isso acarreta, inexoravelmente, um maior tráfego a essas redes. Se esse incremento de demanda não for planejado, o negócio corporativo pode ser prejudicado em função da lentidão ou da suspensão do serviço da rede.

Em vista destes aspectos, os fabricantes de equipamentos buscam inovar e trazer soluções para tais demandas e a evolução dos equipamentos de rede em termos de funcionalidades e capacidade de operação reflete esta condição. Entre essas

soluções está a criação dos switches que efetuam encaminhamento inteligente de tráfego: os chamados switches de camada 3. Assim, será mostrado neste presente trabalho a viabilização e as vantagens que um switch de camada 3.

Os objetivos gerais geral do presente trabalho são é identificar as principais causas dos "gargalos", ou seja, o congestionamento em redes locais e fornecer sugestões de como é possível contornar esses entraves com o uso de switches de camada 3.

Os objetivos específicos estão elencados abaixo:

- Abordar os principais problemas de tráfego encontrados em redes corporativas de médio a grande portes;

- Identificar os tipos de requisição de dados mais usualmente encontrados nessas redes e como tais requisições impactam no tráfego;

- Identificar erros comuns encontrados nas topologias e arquiteturas mais usadas assim como os erros lógicos que ocorrem nessas redes;

- Descrever como funciona um switch camada 3;

- Descrever como situar um switch camada 3 dentro de uma rede tradicional e como esse tipo de equipamento pode mitigar os problemas de tráfego mais comuns.

Os termos apresentados durante a presente monografia exigem certa familiarização com alguns conceitos primordiais de comunicação de dados e de redes de computadores. Embora tais conceitos sejam muitas vezes basais e bem difundidos pela Internet e na documentação especializada e talvez possam ser dispensados às vezes, eles serão abordados e revisados conforme a necessidade antes do aprofundamento dos temas nos capítulos correspondentes.

A metodologia para o presente trabalho incluiu pesquisa bibliográfica com abordagem qualitativa, com introdução de conceitos gerais e com gradual enfoque no tema proposto. A coleta de dados foi realizada com base em conteúdos de livros,

artigos e manuais técnicos dos principais fabricantes do segmento da área de redes de computadores. Os dados obtidos da análise bibliográfica foram apresentados na forma de textos descritivos e figuras.

2 CONCEITOS FUNDAMENTAIS

2.1 REDES: CONCEITOS FUNDAMENTAIS

De acordo com Edwards e Bramante (2009), uma rede de dados é um grupo de computadores ligados uns aos outros por meios físicos de comunicação bem como os protocolos que permitam a comunicação entre eles, ou, ainda, pode ser constituída de redes distintas interconectadas. A figura 1 mostra uma rede de computadores compartilhando aplicações, bem como equipamentos. Estão representados grupos de trabalho (*workgroups*), servidores, impressoras e equipamentos comutadores (*switches*).

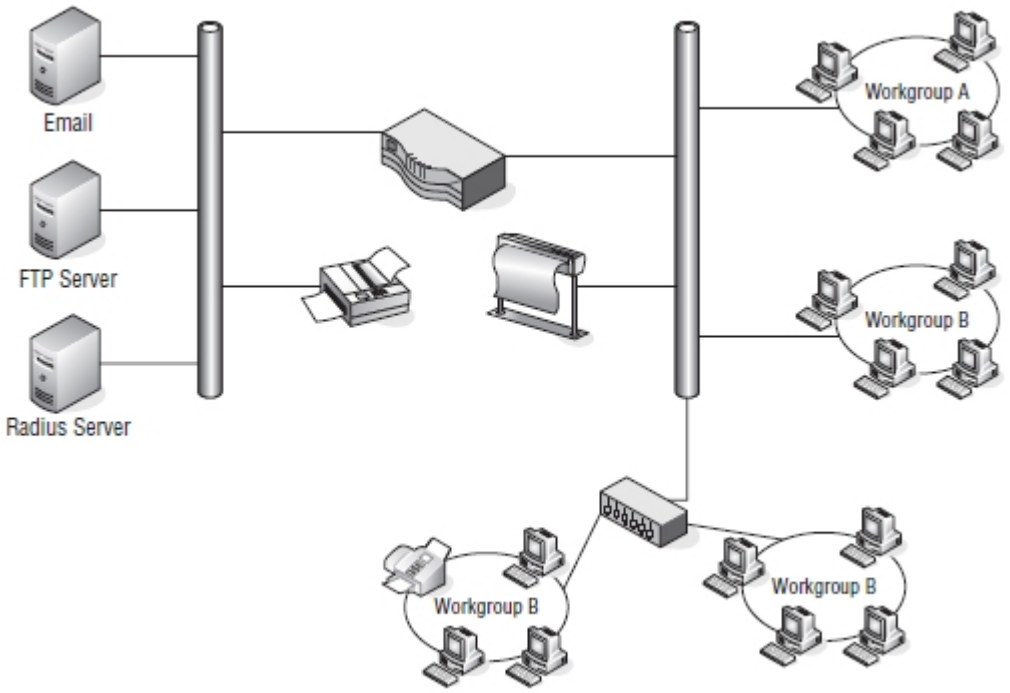

Figura 1: Uma rede de computadores.
Fonte: Edwards e Bramante (2009)

Ainda de acordo com Edwards e Bramante (2009), muitos recursos podem ser compartilhados em uma rede, como aplicações de email, aplicações de processamento de texto, banco de dados e muitos outros recursos.

Tipicamente, as redes podem ser identificadas por seu tamanho, que vão desde pequenas redes locais (LANs) para redes maiores de longa distância (WANs, ou *Wide Area Networks*), muitas delas permanecendo isoladas das outras (EDWARDS e BRAMANTE, 2009).

2.2 REDES LOCAIS - LAN´S

Uma LAN (acrônimo de *Local Area Network*) é uma rede privada que opera dentro e nas proximidades de um único edifício, como uma casa, escritório ou fábrica (TANENBAUM, 2011). Desse modo, ainda de acordo com Tanenbaum (2011), as LANs podem suportar múltiplos protocolos e são amplamente usadas para conectar diferentes tipos de clientes ou *hosts*, como computadores pessoais e eletrônicos de consumo permitindo a eles compartilhar recursos (por exemplo, impressoras) e trocar informações. Quando as LANs são utilizadas pelas empresas, elas são chamadas de *redes corporativas*.

A topologia de muitas LANs cabeadas é construída a partir de ligações ponto-a-ponto. O padrão IEEE 802.3, popularmente chamado de *Ethernet*, é, de longe, o tipo mais comum de LAN cabeada encontrada. A figura 2 abaixo mostra um exemplo de topologia de comutação Ethernet (TANENBAUM, 2011).

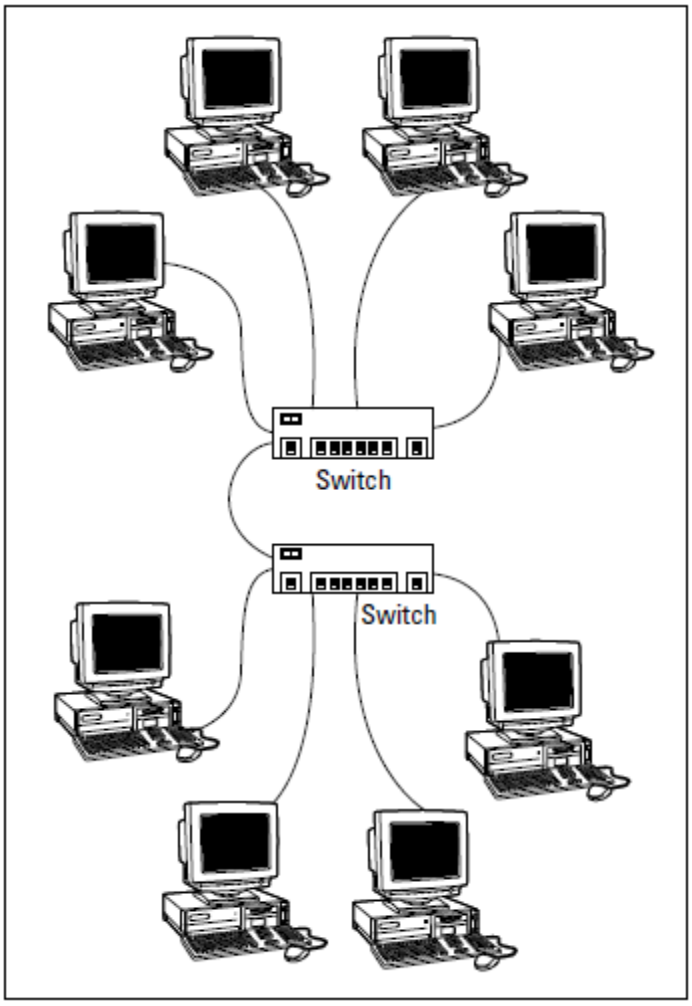

Figura 2 – Exemplo de topologia de LAN comutada com 2 comutadores (*switches*)
Fonte: LOWE (2011)

2.3 MODELO OSI

Em 1977, formou-se um grupo de trabalho para sugerir um modelo em camadas de arquitetura de redes na tentativa de padronizá-la. O esforço conjunto estabeleceu alguns pontos em comum entre os protocolos de comunicação de redes já existentes (EDWARDS e BRAMANTE, 2009).

O modelo OSI (acrônimo de Open Systems Interconnection) oferece uma base de referência para a interconexão (o modo como se comunicam) de sistemas abertos,

alicerçada, estratificada e organizada em sete diferentes camadas (ou *layers*) independentes em suas funções, porém interdependentes no modo como executam a passagem de informações entre si (figura 1). Além disso, cada camada adiciona mais informação aos dados originais durante o processo de envio à camada superior (SOSINSKY, 2009).

Ainda segundo Sosinsky (2009), tal paradigma de camadas provê que essa interconexão pode ser estabelecida entre sistemas heterogêneos e como base para a padronização de protocolos empregados nas diversas camadas. Também pode ser usado como modelo para uma arquitetura de rede, desde as conexões físicas até as aplicações que estão sobre as demais camadas, passando pelas camadas intermediárias de enlace e de rede.

O modelo OSI não é um padrão de rede no mesmo sentido que a Ethernet e TCP/IP são padrões de rede. Pelo contrário, o modelo OSI é uma estrutura em que os vários padrões de rede podem se encaixar (LOWE, 2011).

O modelo OSI especifica quais os aspectos da operação de uma rede podem ser abordados por vários padrões de rede. Assim, em certo sentido, o modelo OSI é uma espécie de padrão de normas (LOWE, 2011).

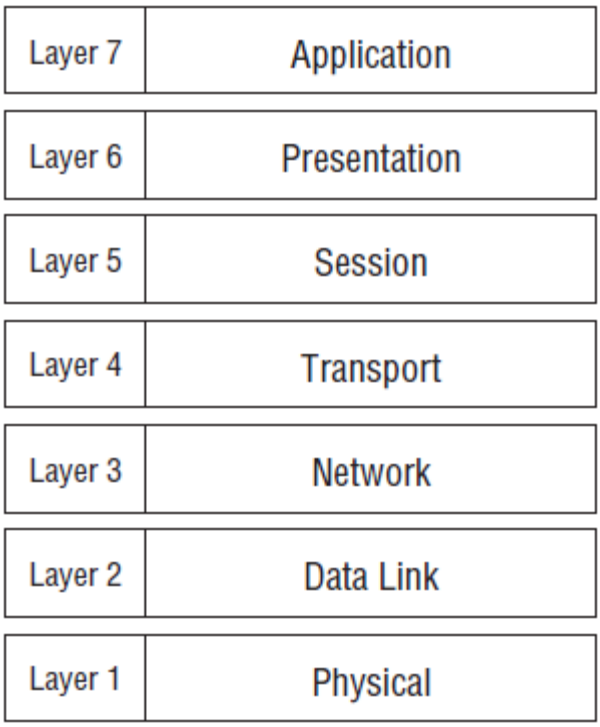

Figura 3 – O modelo OSI e as sete camadas
Fonte: Edwards e Bramante (2009)

Segundo a descrição de Lowe (2011), as primeiras três camadas são às vezes chamadas de camadas inferiores. Elas lidam com a mecânica de como a informação é enviada de um computador para outro através de uma rede.

As demais camadas de 4 a 7 são chamadas camadas superiores. Elas lidam com a forma de como o software aplicativo pode se relacionar com a rede através de interfaces de programação de aplicativos (LOWE, 2011).

A seguir será apresentada breve descrição das camadas do modelo OSI que serão relevantes para o escopo deste documento. A saber: camada física, de enlace de dados e camada de rede. As demais camadas acima serão referenciadas conforme a necessidade de uma explicação sobre elas.

2.3.1 Camada física

Sosinsky (2009) descreve a camada física (camada 1, ou *physical*) como a que controla o meio físico (como por exemplo cabo, rádio, feixe de luz ou algum outro método de transmissão).

Tanenbaum (2011) complementa que a camada física define as especificações elétricas e mecânicas para estabelecimento das conexões de rede e descrevendo a conectividade, a velocidade dos cabos (taxa de informação transmitida por unidade de tempo) e o padrão de pinagem dos cabos (descrevendo inclusive a finalidade de cada pino), além de transmitir as unidades básicas de informação (bits) entre os dispositivos.

2.3.2 Camada de Enlace de Dados

De acordo com Tannenbaum (2011), a camada de Enlace de Dados (camada 2, ou *data link*) padroniza a sincronização da recepção de dados que tiverem sido originadas mesmo a partir de conexões físicas diferentes na camada física. Implementa detecção e correção de erros de transmissão, com retransmissão de quadros, se necessário, sendo assim responsável pelo controle de fluxo das informações. Isso significa que esta camada irá garantir que as mensagens em uma LAN sejam entregues ao dispositivo apropriado usando endereços físicos e irá traduzir as mensagens da camada de rede (camada mais acima) para a Física (camada subseqüente abaixo).

Estes endereços são chamados de endereços MAC (acrônimo de *Media Access Control*), que, segundo Lowe (2011), são inseridos diretamente no *hardware* e compreendem identificações únicas dos equipamentos presentes na rede de acordo com o definido pelo consórcio IEEE e o fabricante do equipamento (adaptador de rede ou switch, por exemplo).

Em linhas gerais, de acordo com Tanenbaum (2011), a camada de Enlace de Dados formata a mensagem em segmentos chamados quadros, ou *dataframes*, que, segundo a definição de Sosinsky (2009), são segmentos de dados empacotados para transmissão em uma rede. Eles são criados via software na camada de enlace de dados onde os dados originais devem ser fragmentados para se alcançar o tamanho de tal formato para o frame. A porção de dados é encapsulada com bits iniciais e finais que representam a que os dados se referem, de onde se originam e qual é seu destino, incluem verificação de erros ou configurações de diagnóstico, entre outra informações. O cabeçalho do padrão Ethernet é um exemplo de dataframe gerado pela camada 2 e é definido padrão IEEE 802.3, conforme a figura 4.

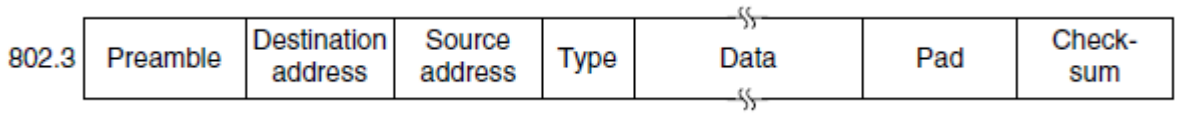

Figura 4 – Dataframe Ethernet

Fonte: Tanenbaum (2011)

Tanenbaum (2011) complementa que a camada de enlace de dados adiciona aos frames cabeçalhos contendo o hardware de destino e o endereço original da fonte de dados. Esse cabeçalho adicional é descartado quando a mensagem chega ao destino.

O processo de segmentação dos *dataframes* impõe uma seqüência na transmissão, e a camada de enlace de dados deve fornecer os meios necessários para recombinar os quadros em dados ao atingir seu destino (SOSINSKY, 2009).

2.3.3 Camada de rede

Segundo Tanenbaum (2011), à camada de rede concerne receber as mensagens dos hosts de origem até que elas cheguem ao seu destino, o que pode exigir que se

executem vários saltos em redes intermediárias ao longo do percurso. Essa função contrasta claramente com a camada de enlace de dados, que tem o objetivo mais modesto de apenas encaminhar os dataframes de um dispositivo localizado em uma ponta do cabeamento a outro em outra ponta.

Como mostrado, cada *host* da rede possui um endereço físico chamado endereço MAC, que é definido de fábrica e atribuído ao dispositivo. Tal endereço é fixo e não pode ser modificado. No entanto, há a possibilidade de se atribuir endereços lógicos aos dispositivos que podem ser usados para se referirem a outros *hosts*. Tais endereços lógicos são chamados de *endereços IP* e são criados e usados pela camada de rede, que os traduz para endereços MAC e vice-versa. Embora o formato exato dos endereços lógicos possa variar dependendo do protocolo em uso nesta camada, a maioria divide tal endereço em uma parte que representa a rede onde o dispositivo se localiza e outra parte que identifica o próprio dispositivo. Dessa forma, o formato do endereçamento é dito roteável, pois o dispositivo que opera na camada de rede pode encaminhar uma determinada mensagem para outra rede caso o *host* de destino não se localize na mesma rede que o *host* de origem (LOWE, 2011).

Lowe (2011) mostra que os endereços IP são números binários de 32 bits e são representados em um formato conhecido como *notação ponto-decimal*. Nesta notação cada grupo de 8 bits – um *octeto* – é representado por seu decimal equivalente. A figura 5 mostra um exemplo de um endereço IP representado por: 192.168.136.28, mostrando a representação em bits, a tradução em algarismos decimais e sua equivalência em notação ponto-decimal. Lowe (2011) denota ainda que deste endereço de 32 bits, há a divisão em 2 partes, o *Network ID* e o *Host ID*, identificando respectivamente a rede e o *host* do dispositivo. A definição do total de *hosts* de uma rede é definida pela *classe* de endereçamento IP, que delimita uma porção maior ou menor de espaço reservado para o total de hosts da rede.

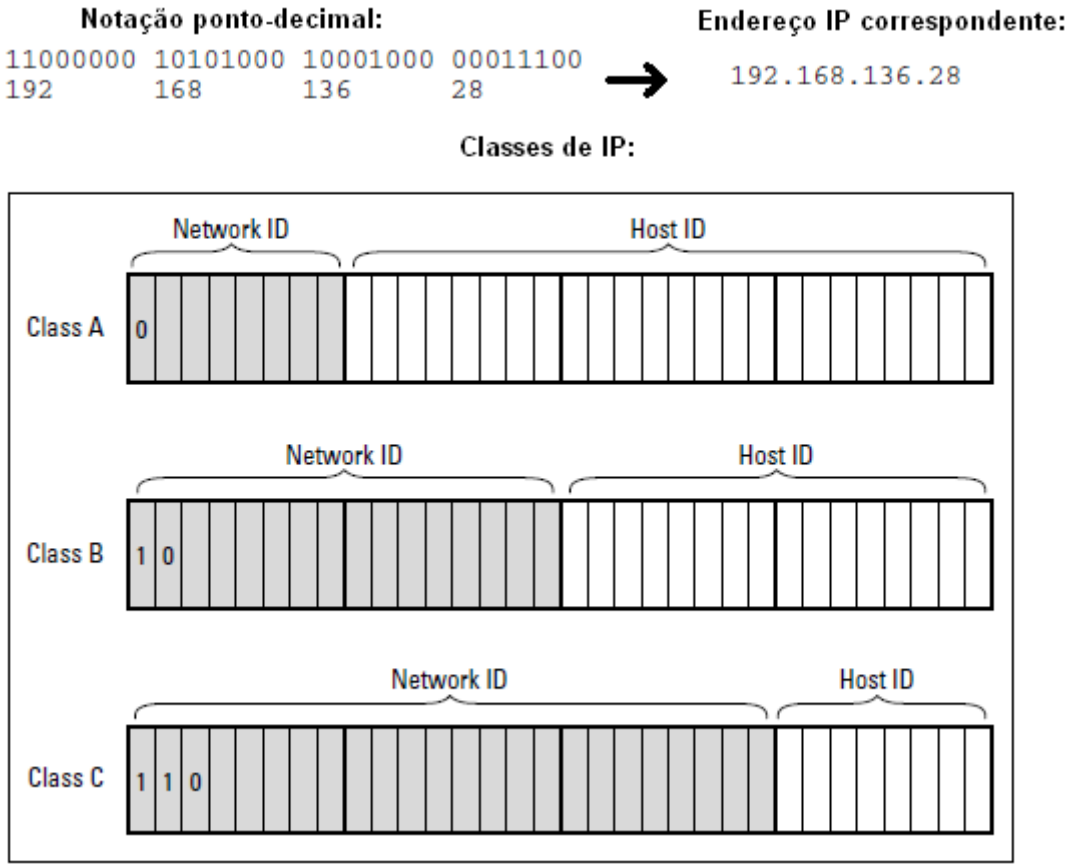

Figura 5 – endereçamento IP e sua representação

Fonte: Lowe (2011)

Na camada de rede é interessante mencionar que conexões ponto-a-ponto conectam pares individuais de *hosts*. Para ir da origem ao destino em uma rede composta por links ponto-a-ponto, mensagens curtas, chamados *pacotes*, em certos contextos, podem ter que visitar primeiro uma ou mais máquinas intermediárias até o destino final (TANENBAUM, 2011).

Segundo a definição de Sosinsky (2009), na comunicação de rede ponto-a-ponto são criadas conexões nomeadas entre dois sistemas na rede: o envio e recebimento de sistemas. Na comunicação ponto-a-ponto, pode haver um ou mais sistemas intermediários que processam o fluxo de dados ao longo do seu percurso pretendido. Muitas redes ponto-a-ponto têm caminhos redundantes através da rede, muitas vezes de comprimento diferentes. Portanto, o papel de roteadores em uma rede ponto-a-ponto é um fator chave para determinar o desempenho da rede de modo global.

O roteamento é necessário quando um host de uma determinada rede necessita enviar pacotes para outro host localizado em outra rede. Neste caso, o *roteador* é usado para encaminhar o pacote à rede destino. Em alguns casos, o pacote pode na verdade ter de viajar através de muitas redes intermediárias a fim de alcançar sua rede de destino final. (LOWE, 2011).

A camada de rede, portanto, fornece uma função de roteamento e de controle que determina qual o caminho que os pacotes de dados usam para trafegar a partir de um ponto a outro ou de uma rede a outra, e proporciona o controle de fluxo necessário para assegurar que uma sub-rede não seja inundada com muitos pacotes em algum momento. O conceito utilizado para definir a comunicação nesta camada é chamado de *sessão*, e a lógica usada para gerenciar sessões depende de rotas específicas determinadas pela função de roteamento (SOSINSKY, 2009).

3 SWITCHES E ROTEADORES

3.3 SWITCHES

Cada computador que utiliza o protocolo Ethernet e se conecta por cabo a um equipamento chamado comutador, ou *switch*. O switch, por sua vez, conecta o restante da rede (LOWE, 2011).

Tanenbaum (2011) explica que um switch possui várias portas, e em cada uma das quais se pode conectar um *host* (definição formal de quaisquer equipamentos de rede, tais como computadores, servidores, impressoras, etc). O trabalho do switch é a retransmissão ou encaminhamento de *frames*, ou quadros, (função conhecida como *switching*) entre computadores que estão ligados a ele, usando o endereço de cada frame para determinar para qual computador enviá-lo.

Segundo Sosinsky (2009), numa rede hierárquica, o nó da raiz está ligado a certo número de nós de nível 1 e a rede continua a se ramificar conforme se afasta da raiz. Uma topologia hierárquica é uma árvore representada de cabeça para baixo, cuja raiz está no nível mais acima da rede, na qual os ramos são lineares e onde a falha de qualquer nó ou conexão a um nó em um galho torna inacessíveis os nós em níveis mais baixos da hierarquia. Uma topologia puramente hierárquica também significa que se um nó em um ramo quer se comunicar com um nó em outro ramo, ele teria que atravessar um caminho até a árvore para o nó raiz e de volta para o nó de destino. Por estas duas razões, apenas pequenas redes podem ser estruturados numa topologia de hierarquia pura. A figura 6 mostra um exemplo de rede hierárquica com 5 camadas, que será detalhada posteriormente.

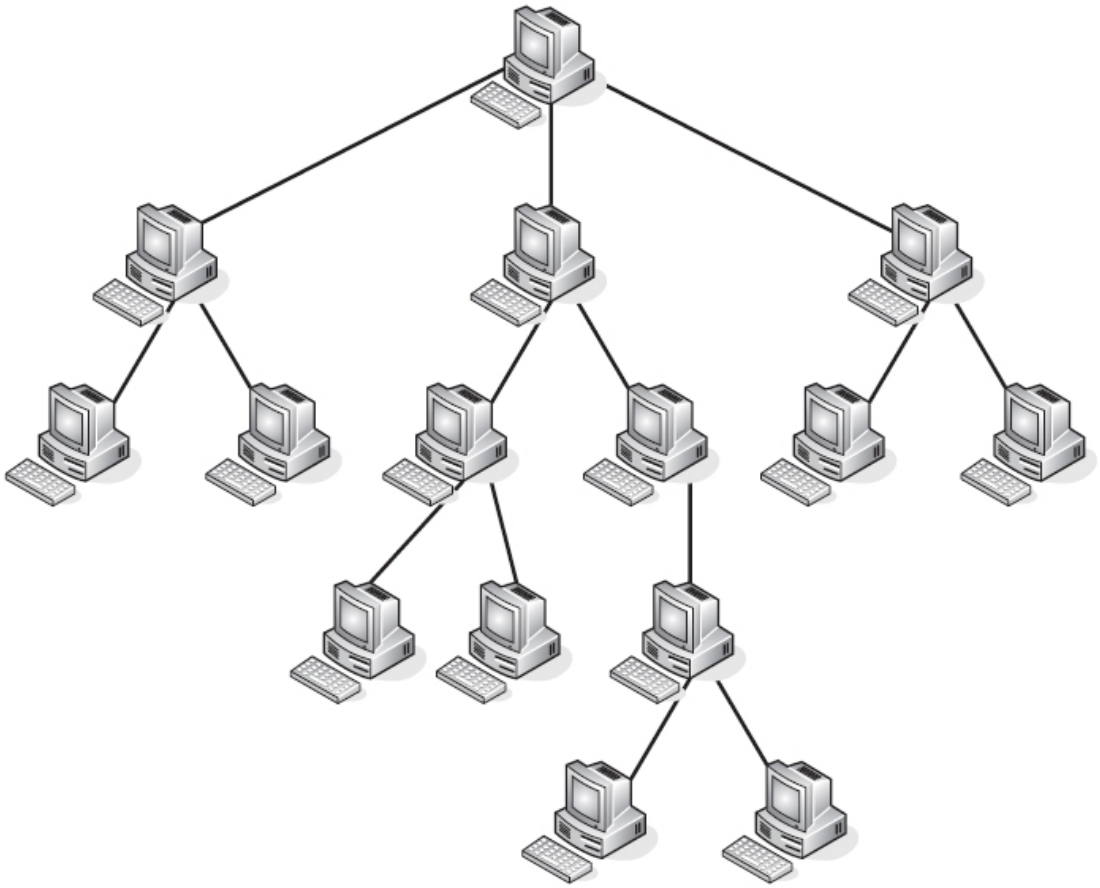

Figura 6 – Exemplo de uma rede hierárquica
Fonte: Edwards e Bramante (2009)

A solução para estes problemas é a construção de ligações cruzadas entre diferentes ramos. Ligações cruzadas fornecem caminhos mais curtos e, portanto, melhor desempenho, e proporcionam certa medida de redundância porque agora existem vários caminhos possíveis de um ponto de origem ao destino através da rede para a maioria das conexões, eliminando o ponto de falha de uma ramificação da rede hierárquica (SOZINSKY, 2009).

Neste sentido, um switch é um dispositivo ativo que conecta dois segmentos de rede em conjunto em um ou mais níveis do modelo de rede OSI. Um switch atua encaminhando pacotes sobre a camada 2 (camada de enlace de dados) e, diferentemente de um *hub*, que basicamente age como um repetidor de sinal, apenas retransmitindo o sinal recebido da origem, o switch tem a capacidade de analisar os cabeçalhos dos *dataframes* da camada 2 e encaminhá-los baseado em endereços MAC (SOZINSKY, 2009).

O *switch* permite uma hierarquização da rede, atuando como elemento centralizador dos demais *hosts*. Como mostrado na figura 4, os switches possuem número variado de portas (de 4 a 48 portas, normalmente), cada qual conectando um host distinto (DLINK, 2013).

Figura 7 – Switches Ethernet com número de portas variado

Fonte: Dlink (2013)

Os switches também podem ser conectados a outros switches, permitindo assim a ampliação do total de número de pontos conectados na rede. A essa conexão dá-se o nome de *cascading*, ou *cascateamento* de switches (figura 8). Assim, cada switch cascateado cria um entroncamento distinto em uma rede hierárquica (PRATICALLY NETWORKED, 2013).

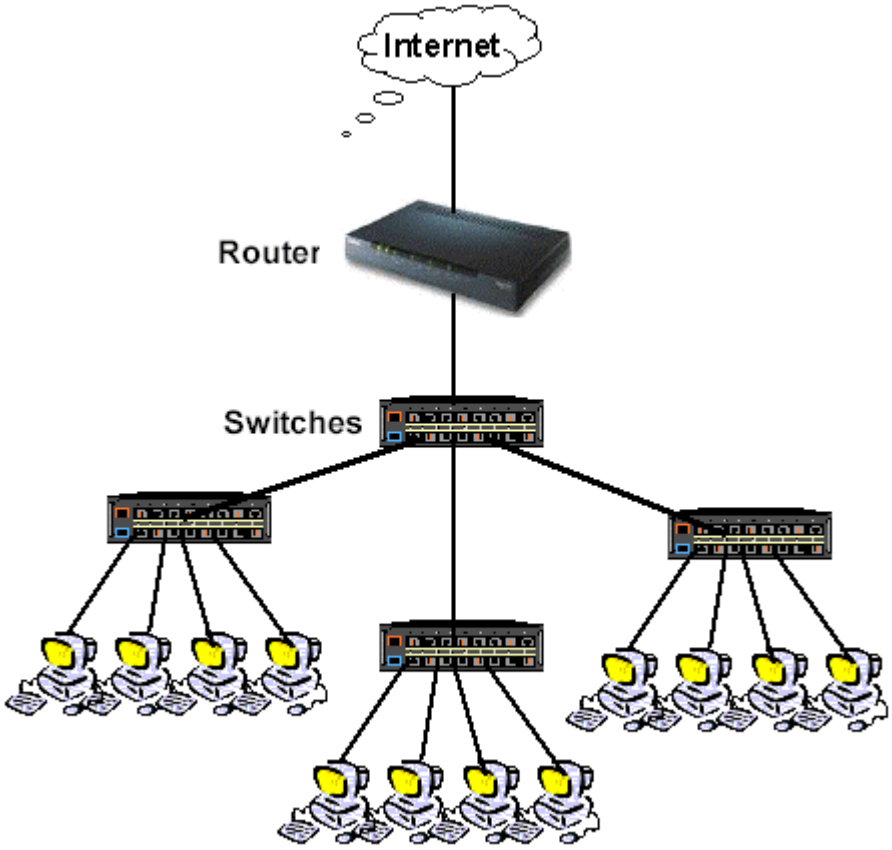

Figura 8 – Exemplo de rede com switches cascateados
Fonte: Pratically Networked (2013)

3.2.1 Switches gerenciados e não gerenciados

Os switches podem ser gerenciados ou não-gerenciados. Um switch não gerenciado não pode ser configurado na rede. Switches gerenciados geralmente incluem interface SNMP (Simple Network Management Protocol) implementada dentro de uma console (interface de usuário com linha para inserção de comandos) ou então uma interface que permite o gerenciamento a partir de um navegador (*browser*). Um switch do tipo smart é aquele que inclui um pequeno conjunto de definições configuráveis e se diferencia de um switch plenamente gerenciável que possui funções como a capacidade de criar e armazenar diferentes configurações (SOSINSKY, 2009).

De acordo com Sosinsky (2009), ao se abordar as definições de um switch, considera-se as seguintes características:

- Portas: o número de portas de um switch e outras funções avançadas, como a capacidade de priorizar o tráfego de determinadas portas;

- Velocidades: a velocidade da porta em termos da taxa de dados por unidade de tempo (mais exatamente em bits por segundo, ou *bps*) e a capacidade de se multiplicar a velocidade de uma conexão ao se somar as capacidades de cada porta pode afetar o desempenho total do switch;

- Agregação de links: a capacidade de enviar dados através de múltiplas conexões para o mesmo destino;

- Capacidade de SNMP (Single Network Management Protocol): ou capacidade de participar na descoberta e gerenciamento de rede, ou seja, do switch poder ser visível a partir de um host e poder ser gerenciado e configurado a partir dele;

- Filtragem: a capacidade de tráfego de segmento com base na identificação física dos dispositivos (por exemplo, a filtragem de MAC). O Network Address Translation, ou NAT, é considerada uma função de um firewall ou um roteador e, geralmente, não é encontrado em switches, embora haja exceções a esta regra;

- Network Access Control: capacidade de um switch de proporcionar uma função de ponte entre duas redes diferentes. Isso é importante, por exemplo, para switches sem fio que fornecem acesso a redes Wi-Fi gratuito;

- VLAN (de Virtual LAN, ou LAN Virtual): A capacidade de criar um grupo lógico de sistemas constituídos por um único domínio de broadcast. Ou seja, dentro de uma LAN fisicamente constituída, o switch é capaz de segmentá-la em 2 ou mais redes separadas, mesmo que fisicamente elas estejam unidas. Dessa forma, um switch com 24 portas pode ser segmentado em 2 VLANs com 12 hosts cada, por exemplo, de modo que os hosts possam somente enxergar os demais hosts dentro de sua

mesma VLAN. A vantagem deste tipo de abordagem é que ao segmentar redes em domínios de broadcast é possível isolar o tráfego e reduzir a utilização da rede.

Sosinsky (2009) afirma que, em sentido mais amplo, pode-se afirmar que o switch é um elemento de uma LAN que atua essencialmente encaminhando *dataframes* em camada 2, mas também com funcionalidades de camadas superiores, como será descrito à frente.

3.3 ROTEADORES

Sosinsky (2009), apresenta a comutação e o roteamento como dois métodos para encaminhar dados em uma rede. Pondera, porém, que o roteamento refere-se a métodos que são executadas em camada de rede (camada 3). Um roteador (do inglês *router*) direciona o tráfego de rede baseado em endereços lógicos atribuídos (endereços IP), enquanto um switch usa apenas o ID de hardware (endereço MAC). Por isso, os roteadores podem determinar quando diferentes redes estão em uso, enquanto um switch não tem a mesma capacidade, o que faz com que os roteadores sejam menos propensos a erros do que switches.

Como regra geral, usa-se switches para conectar segmentos de rede e roteadores para conectar redes diferentes (conforme a figura 9 que mostra o roteador ligando 2 tipos de redes distintas, *Token Ring* e *Ethernet* e também à Internet). Switches são dispositivos de baixo custo, mais caros que os hubs ou repetidores, mas menos caro do que roteadores (SOSINSKY, 2009).

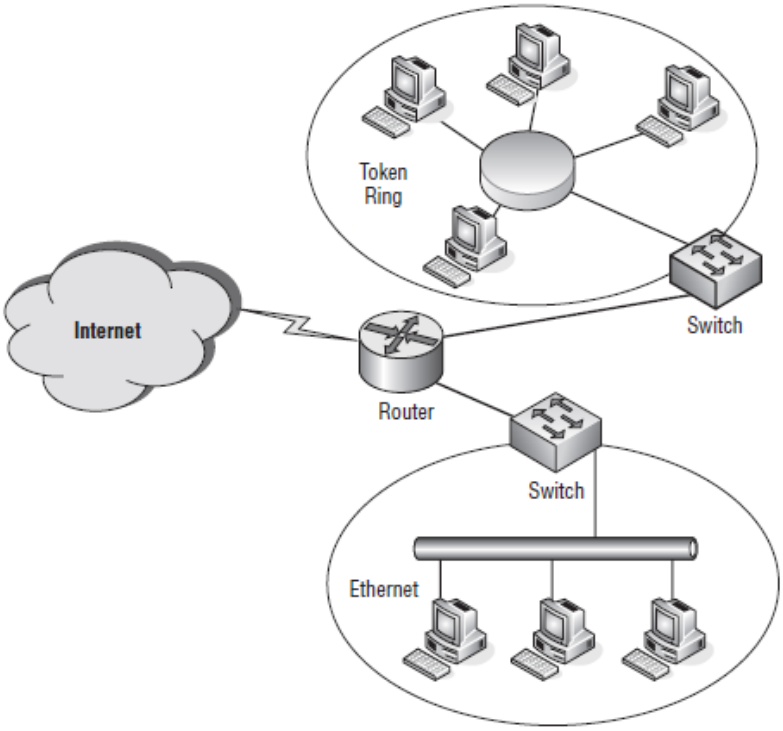

Figura 9 – Roteador conectando duas redes distintas e à Internet
Fonte: Edwards e Bramante (2009)

Os roteadores, diferentemente dos switches, possuem como funcionalidade principal a capacidade de conectar 2 tipos distintos de redes. Pode-se definir mais informalmente, conforme a seguinte afirmação: os roteadores são inteligentes o suficiente para saber como obter dados a partir de uma rede Token Ring e transmiti-los à uma rede Ethernet, sem corrupção dos dados originais. Os roteadores suportam muitos protocolos e padrões que permitem muito mais flexibilidade na sua implementação (EDWARDS e BRAMANTE, 2009).

Como um roteador é um dispositivo que opera na camada de rede (camada 3) do modelo OSI, ele trabalha com os pacotes de rede em um nível superior. Em particular, um roteador pode examinar o endereço IP dos pacotes que passam por ele. Assim, como os endereços IP têm tanto um endereço de rede e um endereço de host, um roteador pode determinar de que rede uma mensagem se origina e para qual rede se destina. Um protocolo é considerado roteável se usa endereços que incluem uma parte de rede e uma parte de host. Os protocolos que utilizam endereços físicos (mais especificamente os endereços MAC) não podem ser roteados porque tais endereços físicos não indicam de qual rede este dispositivo

pertence. A principal diferença entre encaminhamento (*forwarding*, que os switches executam) e roteamento (routing) está justamente na inclusão do endereço de rede ao dataframe de camada 2, que assim passa a ser denominado *pacote*, e à capacidade do roteador de poder interpretar tais pacotes e encaminhá-los de acordo com sua origem e destino dentro da LAN (LOWE, 2011).

Neste aspecto, um roteador é um *gateway*, que formalmente é definido como o nó da rede que opera como tradutor de protocolos entre 2 tipos diferentes de rede, ou como no exemplo dado anteriormente, entre uma rede Token Ring e uma rede Ethernet, que individualmente possuem protocolos diferentes e modos de comunicação distintos. Isso porque ambas as redes suportam o mesmo protocolo de camada 3, não importando, assim, se ambas as redes possuam diferentes protocolos entre si nas camadas 1 e 2 do modelo OSI (Tanenbaum, 2011).

Os roteadores também são capazes de se comunicar com outros roteadores e informações caminho de compartilhamento, então quando um pacote é recebido, ele pode ser enviado para seu destino sobre o melhor caminho possível. Os roteadores executar algoritmos para ajudar a determinar o melhor caminho, e eles compartilham essas informações entre si. Os roteadores assim garantem o recebimento dos dados para onde devem ser direcionados os pacotes (LOWE, 2011).

Edwards e Bramante (2009), explicam que os roteadores mantêm tabelas que ajudam a determinar qual o melhor caminho de um destino de roteamento. A tabela de roteamento contém informações que mostram quais sub-redes o roteador tem aprendido e o caminho para o próximo nó (próximo salto) que leva para o endereço IP de destino. Ainda segundo Edwards e Bramante (2009), a tabela de roteamento é capaz de calcular e definir uma métrica ou o custo para um destino para auxiliar nas decisões de roteamento. As entradas na tabela de roteamento podem ser configuradas (definição de rotas de modo estático) ou aprendidas dinamicamente através de um protocolo de roteamento como RIP ou OSPF, conforme será descrito adiante. A figura 10 mostra um exemplo de uma tabela de roteamento.

```
Active Routes:
Network Destination Netmask Gateway Interface Metric
 0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.104 1
 127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1
 192.168.1.0 255.255.255.0 192.168.1.104 192.168.1.104 1
 192.168.1.104 255.255.255.255 127.0.0.1 127.0.0.1 1
 192.168.1.255 255.255.255.255 192.168.1.104 192.168.1.104 1
 224.0.0.0 224.0.0.0 192.168.1.104 192.168.1.104 1
 255.255.255.255 255.255.255.255 192.168.1.104 192.168.1.104 1
Default Gateway: 192.168.1.1
```

Figura 10 – Exemplo de uma tabela de roteamento

Fonte: Edwards e Bramante (2009)

4 TOPOLOGIAS DE LANS EM FORMATO ESTRELA E REDES HIERÁQUICAS

4.1 TOPOLOGIAS MAIS COMUNS E TOPOLOGIA EM ESTRELA

Pode-se caracterizar as redes baseadas em sua forma ou topologia. Topologias comuns são as baseadas e bus (barramento) ou correntes; estrelas (ou hub), e raios, anéis e malhas. As diversas topologias existentes podem ser combinadas umas com outras (LOWE, 2011).

Uma LAN baseada no padrão Ethernet, definida pelo padrão 802.3 do IEEE, é basicamente uma rede local baseada em topologia de estrela que inclui um elemento central (switch) que atua conectando todos os demais hosts desta rede (figura 7). Nesta topologia todos os dados que trafegam pela rede devem fluir através deste nodo central (LOWE, 2011).

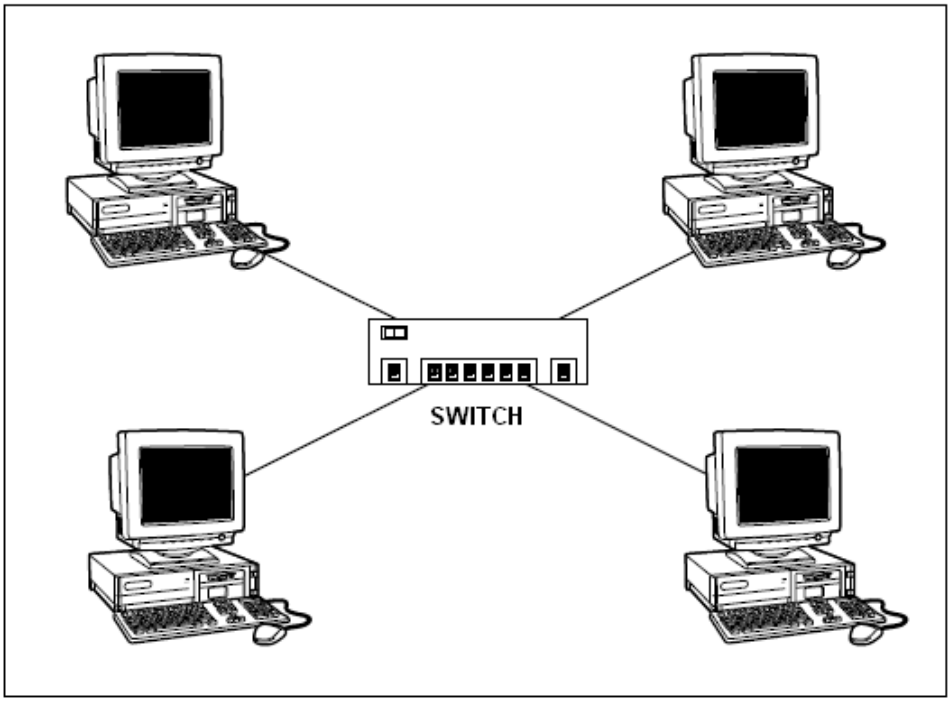

Figura 11 – Exemplo de topologia em estrela

Fonte: Lowe (2011)

Na topologia em estrela os hosts estão conectados ao elemento central e a LAN, como um todo, está limitada em número de pontos ao total de portas do switch. Para se estender o total de portas de uma LAN é necessário se adicionar mais switches conectando-os aos demais. Isso pode levar à criação de uma estrutura em árvore (também chamada hierárquica) da LAN (EDWARDS e BRAMANTE, 2009).

Uma rede hierárquica começa com um nível mais alto, ou raiz, onde um único nó está ligado a nós em um segundo nível da hierarquia. Nós de segundo nível se conectam a um ou mais nós no terceiro nível, e cada nível se estende ainda mais. Portanto, deve haver pelo menos três níveis em uma rede hierárquica (figura 12), assim como dois níveis para se definir uma topologia em estrela (SOSINSKY, 2009).

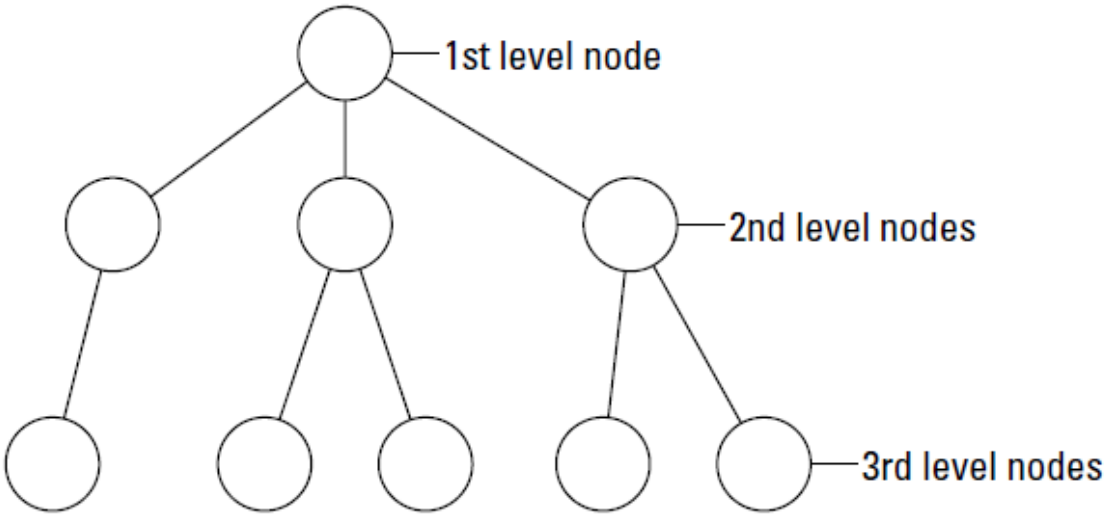

Figura 12 – representação da árvore formada a partir da rede hierárquica
Fonte: Sosinsky (2009)

Desta forma, o que ocorre na prática é a criação de uma topologia híbrida, formada de elementos organizados em forma de estrela e outros de forma hierárquica. Neste tipo de topologia, cada nó da hierarquia de árvore pode ser considerado um centro a partir do qual saem ramificações. Cada nível seguinte na hierarquia irradia outras ramificações. Não há barramento comum que liga as estrelas diferentes, apenas há

ligações ponto-a-ponto existentes nesta topologia (SOSINSKY, 2009). A figura 13 ilustra uma rede hierárquica:

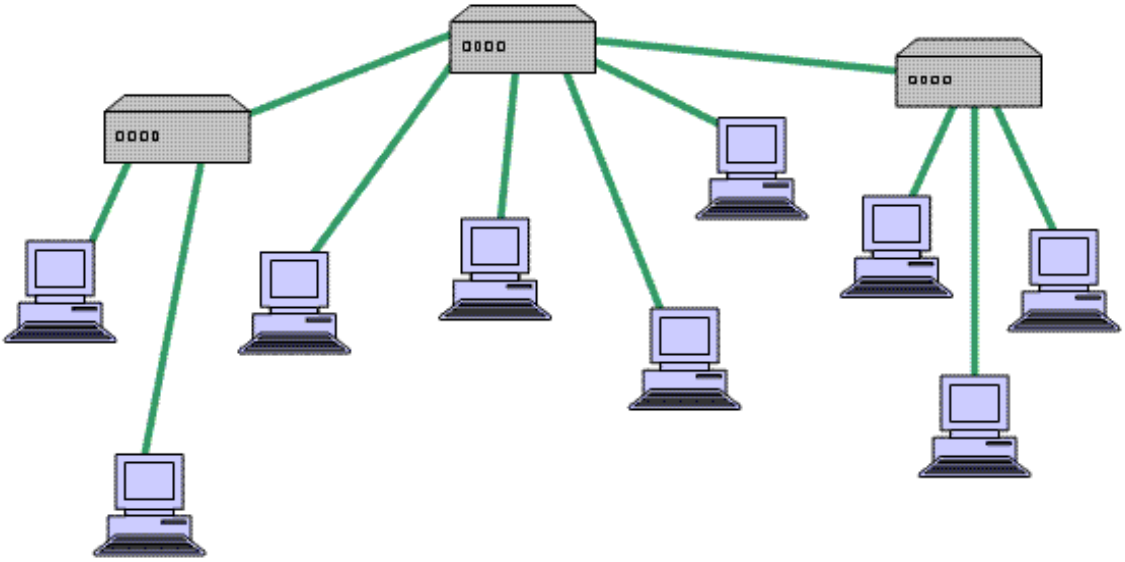

Figura 13 – Rede hierárquica
Fonte: Hinetworld (2012)

A figura 13 mostra um switch localizado no centro da topologia e a partir dele 6 ramificações: 2 direcionando a outros switches e 4 para hosts, enquanto que os demais switches se ramificam para conectar somente hosts (HINETWORLD, 2012).

Edwards e Bramante (2009) descrevem que o tipo de topologia hierárquico supõe que os dados trafeguem sempre do nível inferior ao nível superior, ou seja, das ramificações para a raiz. Assim, o tráfego deve necessariamente passar pelo elemento que conecta os hubs em um determinado segmento da rede. Uma conseqüência desta obrigatoriedade é que em determinadas situações, em LANs que possuem um número considerável de pontos e ramificações a partir do nodo central, há um prejuízo em termos de desempenho da rede. Evidentemente, a saída para esse tipo de limitação é conectar 2 switches que estejam em um mesmo nível de ramificação, criando assim atalhos que possibilitem que os dados de um host de origem cheguem ao destino mais rapidamente, conforme mostra a figura 14.

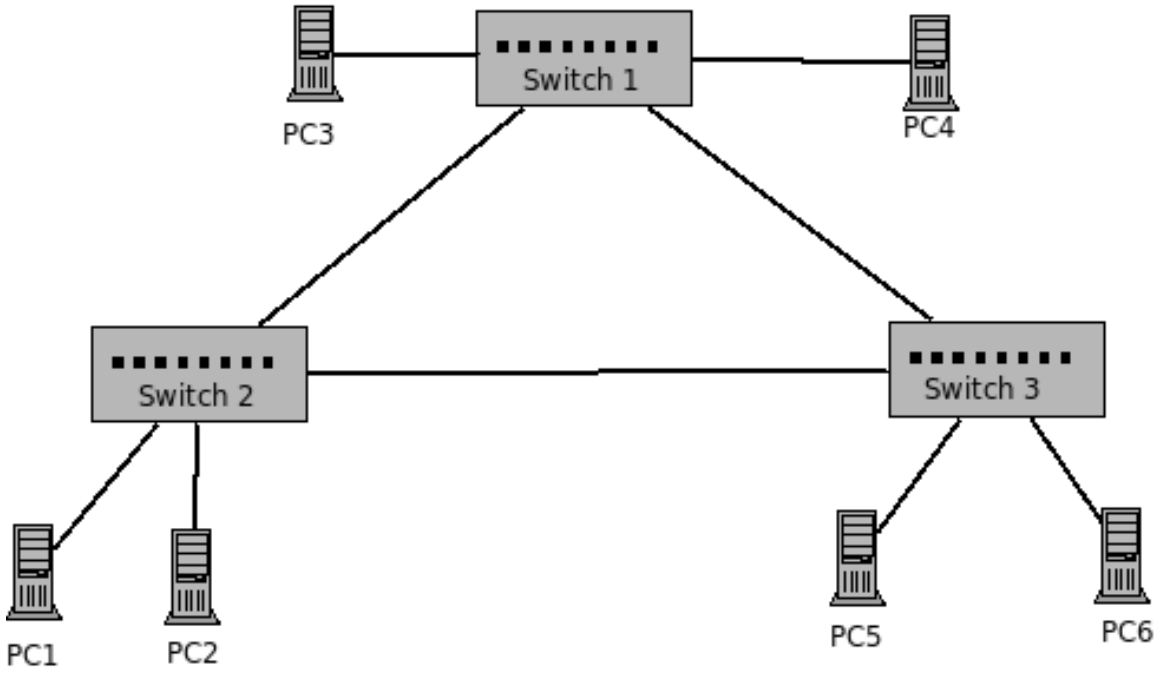

Figura 14 – Exemplo de formação de anel (ou *loop* entre 3 switches)
Fonte: IFSC (2013)

O que se nota é que os switches 1, 2 e 3 formam um anel, ou *loop* entre si. A princípio essa configuração é intencional e praticável, pois em LANs grandes pode ser desejável ter enlaces redundantes, para evitar que a interrupção de um enlace isole parte da rede. A existência de interligações alternativas, portanto, é algo que pode ocorrer em uma rede local, seja por acidente ou com a finalidade de conferir algum grau de tolerância a falhas na infraestrutura da rede, mas em certas situações esse tipo de conexão pode acarretar em uma *inundação* da rede (IFSC, 2013).

Conforme visto, os switches encaminham pacotes baseados em endereços MAC. Existem ocasiões nas quais os switches necessitam enviar requisições a todos os hosts. Essas requisições utilizam um recurso que leva o nome de *broadcast*. Enquanto essas requisições de broadcast são executadas em redes plenamente hierárquicas (sem anéis) ela é feita normalmente (EDWARDS e BRAMANTE, 2009). Ocorre que se há um anel presente na rede, os switches que o compõe recebem a requisição de *broadcast* e passam a retransmiti-la indefinidamente, de modo que a rede de passa a ficar congestionada como um todo e ocorre o que se chama de *broadcast storm*, ou o termo *inundação* mencionado anteriormente, que é o efeito

dos infinitos redirecionamentos das requisições. Essa condição acarreta em consumo de recursos de rede e a supressão da capacidade da rede de transportar o tráfego convencional e é ainda agravada quando há mais anéis deste tipo em sequência (LOWE, 2011).

Para contornar a situação acima, fabricantes de equipamentos de redes criam mecanismos de detecção de anéis, bloqueando automaticamente uma das portas que participa do anel. No entanto, somente bloquear o acesso às portas do switch não é suficiente, visto que a porta bloqueada ficaria indisponível até que o anel fosse desfeito (ANGELESCU, 2010). Em vista disso, desenvolveu-se o protocolo STP (*Spanning Tree Protocol*), que assegura para a rede uma topologia livre de anéis, bloqueando o tráfego de uma ou mais portas dos switches que compõe a rede. O protocolo se originou da teoria dos grafos que prevê que em estruturas conectadas que formam anéis podem ser reduzidas a uma única estrutura de árvore que elimina os anéis, mas ainda abrange os nós desta rede, permitindo que os dados possam percorrer todos os pontos que formam os anéis, sem incorrer em redundância de links (EDWARDS e BRAMANTE, 2009).

4.2 REDES HIERÁRQUICAS EM 3 NÍVEIS

Por razões de segurança e desempenho, um modelo de arquitetura de rede corporativa difundido em larga escala é o modelo hierárquico em 3 níveis, ou camadas (CISCO, 2008).

Muito diferente que o modelo de referência OSI, este modelo é usado como a base para o desenho. O artigo fornece uma visão geral dos papéis e responsabilidades de cada uma das três camadas do modelo (CISCO, 2008).

Enquanto o modelo OSI fornece uma forma como os diferentes sistemas comunicam através de redes, o modelo Cisco hierárquico é um modelo de tipos que define como as redes devem ser projetadas em camadas. Cada camada é destinada a ter os

seus próprios papéis e responsabilidades, mas o objetivo é criar uma rede que oferece alto desempenho e gerenciável. Embora este modelo tenha sido projetado pela Cisco, seu uso pode ser adaptado para conter switches ou roteadores de qualquer fornecedor (EDWARDS e BRAMANTE, 2009).

O modelo é composto por três camadas, incluindo Núcleo (do inglês *core*), Distribuição e Acesso. O diagrama da figura 11 mostra cada uma destas camadas em relação ao outro (WEBPRONEWS, 2013).

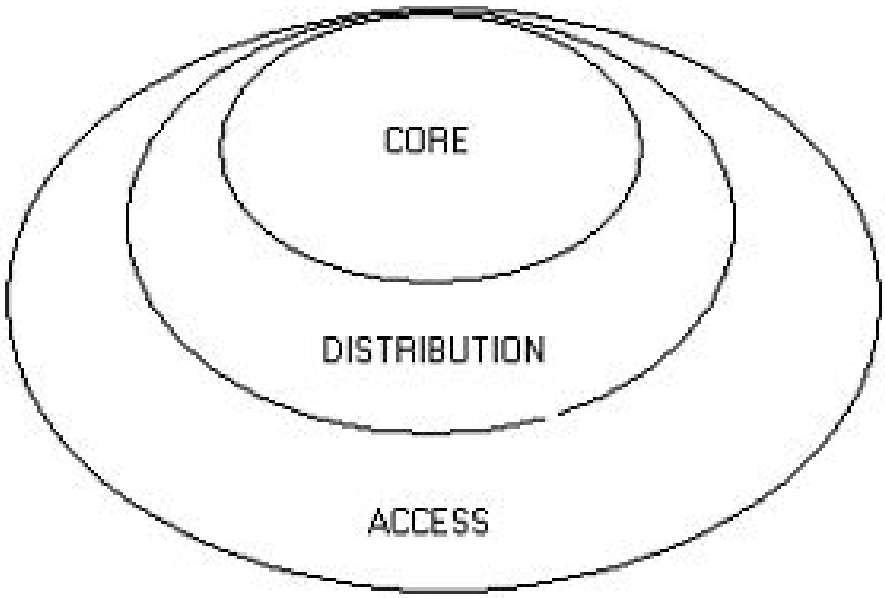

Figura 15 – as 3 camadas do modelo hierárquico (*core* – *ou* núcleo – distribuição e acesso)
Fonte: Webpronews (2013)

Cada camada do modelo tem um nível de funcionalidade, em termos do que as capacidades devem ser implementadas neste nível, e com particular ênfase em como essa camada deve atuar. A camada de núcleo da rede (ou *core*) seria considerada ao longo das mesmas linhas como a espinha dorsal – provendo alta velocidade e redundância. A camada de distribuição conteria roteadores e switches intermediários. A camada de acesso é, literalmente, onde os usuários se conectam ao switch local. Embora esta seja uma visão simplificada da rede, ela fornece uma visão geral de alto nível (WEBPRONEWS, 2013).

Aprofundando um pouco mais a definição, cada camada do modelo possui suas próprias funcionalidades. Este é um modelo, e, como tal, nem todas as redes necessariamente possuirão a mesma arquitetura – muitas delas, especialmente as redes menores, terão desenho muito diferente. Em vez disso, é possível pensar neste modelo como aquele que apresenta as melhores práticas para garantir que a confiabilidade e escalabilidade da rede e que atende aos requisitos de desempenho necessários (EDWARDS e BRAMANTE, 2009).

A figura 16 mostra um exemplo de implementação de uma rede hierárquica em 3 camadas:

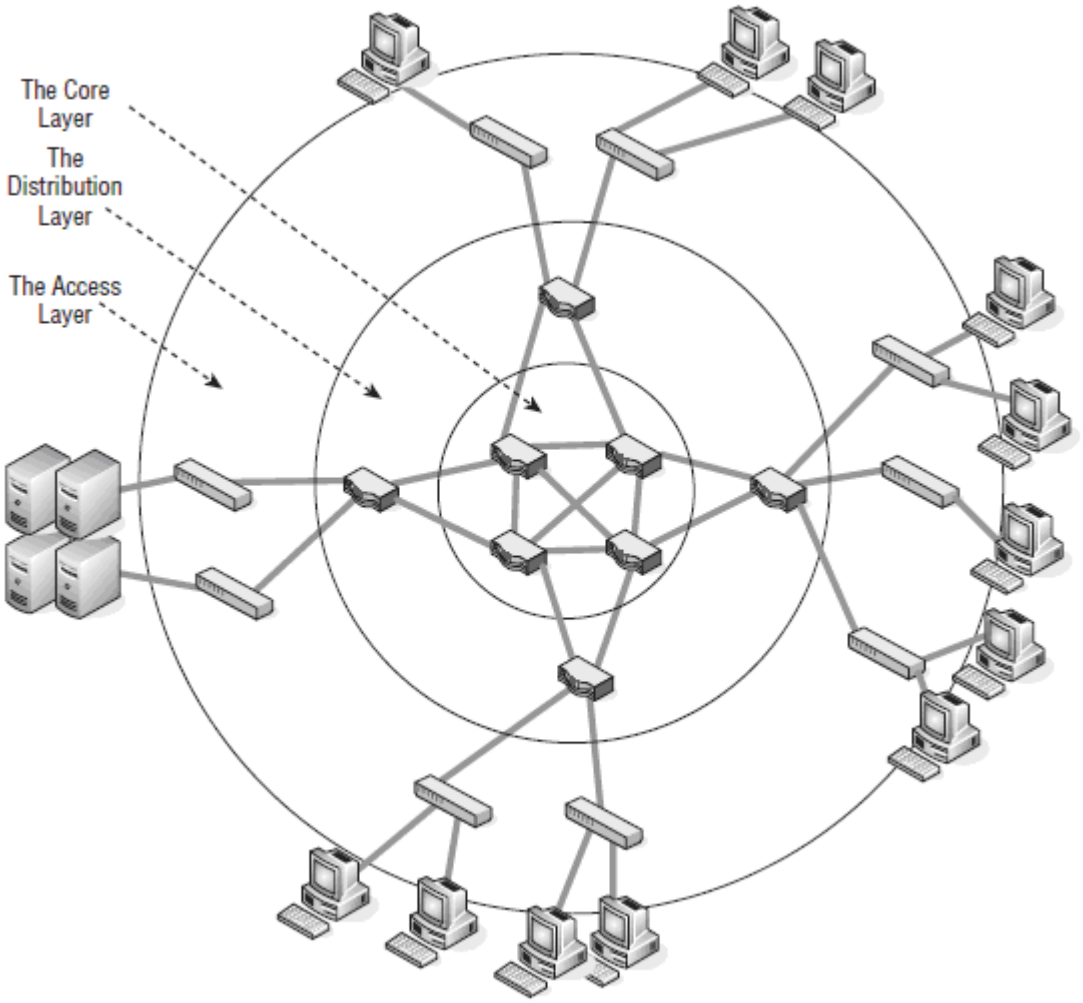

Figura 16 – Implementação em uma rede hierárquica em 3 camadas

Fonte: Edwards e Bramante (2009)

4.2.1 Camada *Core*

Segundo Edwards e Bramante (2009), a responsabilidade da camada *core* é o de atuar como uma espinha dorsal (*backbone*) comutada alta velocidade e oferecer conectividade para WANs, bem como aos serviços de Internet.

É na camada *core* que diferentes redes se unem. Por essa razão é chamada de *backbone* (espinha dorsal) da rede. Deve ser esperado que a camada *core* possua alta velocidade com grande largura de banda, alta disponibilidade, oferecendo um grau de redundância, fornecendo caminhos diversos com conexões e links redundantes a fim de que o tráfego possa fluir sem impedimentos. Ou seja, mesmo se um link cair, haverá um caminho alternativo para o tráfego (ANGELESCU, 2010).

Note-se que para a essa camada é esperado comutar o tráfego, e não roteá-lo. O roteamento pode afetar o desempenho, principalmente porque cada quadro precisa ser recriado à medida que passa através de cada roteador. Neste sentido a comutação fornece um desempenho muito superior, principalmente por causa de um quadro pode trafegar por todo o *backbone* sem a necessidade de ser recriado em cada switch, o que não significa que o quadro não é inspecionado em cada switch, mas tudo fica em camadas OSI 1 e 2, em vez de ter que ser considerado na camada 3. A camada de núcleo é geralmente composta de um número relativamente pequeno de switches de alto desempenho (WEBPRONEWS, 2013).

Em geral, é necessário de que o tráfego somente flua através da camada core seja o que está sendo trafegado entre diferentes dispositivos de camada de distribuição. Um projeto deve prever que o fluxo do tráfego sobre a camada de núcleo, quando não é necessário, não irá fornecer o melhor desempenho. Para efeito, o núcleo também nunca deve ser usado para implementar filtros de tráfego, tais como listas de acesso - estes devem ser implementadas nas demais camadas (WEBPRONEWS, 2013).

Para resumir (WEBPRONEWS, 2013), o Core deve:

- Ser usado para fornecer comutação de alta velocidade;
- Fornecer confiabilidade e tolerância a falhas;
- Ser ampliado usando equipamentos mais poderosos, e não com a adição de mais equipamentos.

Adicionalmente, de acordo com Angelescu (2010), o core pode possui equipamentos que ofereçam:

- Fontes de alimentação redundantes;
- Sistemas de refrigeração redundantes.

4.2.2 Camada de distribuição

A camada de distribuição atua como uma camada intermediária, ligando as camadas de core e as camadas de acesso e é geralmente onde as funções de roteamento entre os *hosts* da camada de acesso, em uma rede bem projetada, são encontradas. Um exemplo do tipo de interconexão aqui inclui entre os diferentes tipos de mídia, tais como Ethernet e Token Ring. A camada de distribuição também é onde as políticas são normalmente implementadas usando listas de acesso (WEBPRONEWS, 2013).

De acordo com Angelescu (2010), as funções principais desempenhadas por switches e roteadores na camada de distribuição são:

- Encontrar a melhor rota para os pacotes;
- Filtrar pacotes;
- Interconectar LANs;
- Conectar as LANs às WANs;
- Retransmitir os pacotes à camada *core*, se necessário;
- Oferecer políticas de segurança à rede.

É também aconselhável na camada de distribuição implementar a função de roteamento entre VLANs. Incluindo aí o uso de switches de camada 3. (ANGELESCU, 2010).

Para se ter uma idéia da função da camada de distribuição, é necessário entender que geralmente há uma grande quantidade de roteamento em uma rede. Clientes em uma sub-rede ou VLAN podem precisar falar com os servidores em outra sub-rede ou VLAN. Em alguns casos, este tráfego é localizado, como no caso de arquivos de departamentos ou servidores de banco de dados. No entanto, muitas vezes há servidores que precisam ser acessados por muitas sub-redes dentro de um mesmo local, como servidores de correio. A camada de distribuição é responsável por essa função de roteamento (WEBPRONEWS, 2013).

4.2.3 Camada de Acesso

A camada de acesso atua como o ponto onde os hosts se conectam ao restante da rede, geralmente ligando em switches. Os hosts encontrados nesta camada geralmente são pontos de acesso sem fio, repetidores e switches de camada 2 (EDWARDS e BRAMANTE).

O diagrama da figura 17 mostra como uma rede típica pode ser configurada para explicar o modelo de projeto de rede hierárquico Cisco. É bom frisar que a camada de switches centrais pode conter equipamentos que estão geograficamente dispersos, e que a camada de roteadores de distribuição pode ser ligado ao núcleo através de um link de WAN semelhante (WEBPRONEWS, 2013).

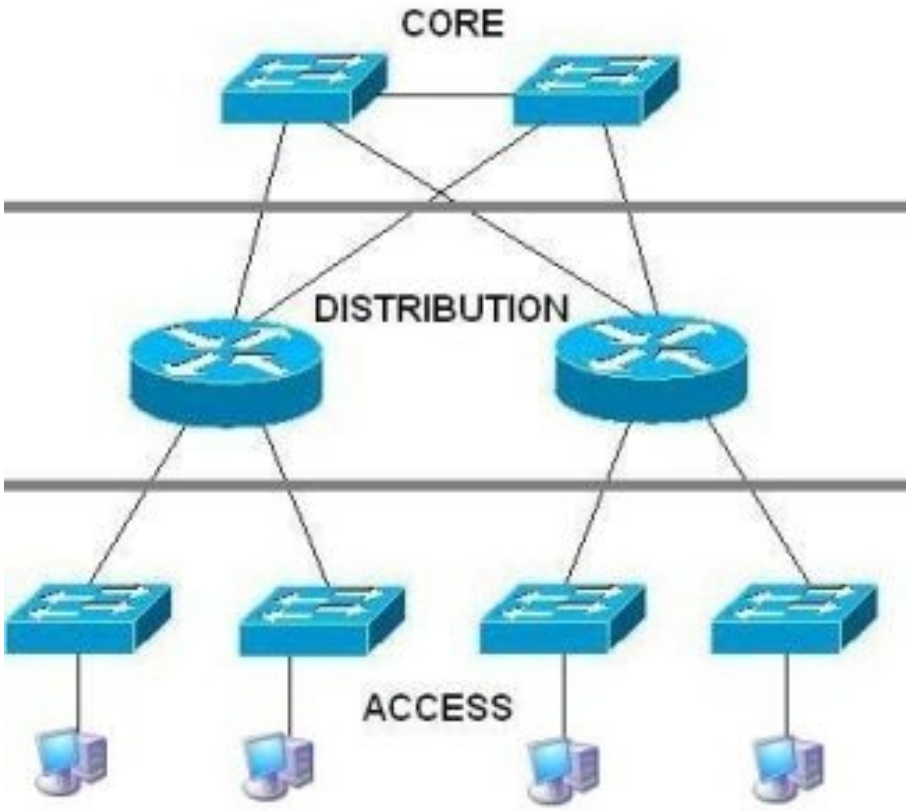

Figura 17 – Exemplo de rede hierárquica em 3 camadas

Fonte: Webpronews (2013)

5 SWITCHES DE CAMADA 2 E CAMADA 3: DIFERENÇAS

O capítulo anterior mostrou que de forma geral as corporações adotam modelos similares ao modelo hierárquico de 3 camadas, com variações. Em determinados aspectos, as diferentes camadas apresentam equipamentos com funcionalidades e capacidades diferentes. Como visto, a camada de core apresenta equipamento com alta capacidade de encaminhamento de tráfego, a camada de distribuição é responsável pelo roteamento inteligente do tráfego e a camada de acesso faz o papel de conexão entre os usuários e o restante da rede (EDWARDS e BRAMANTE, 2009).

As definições mostradas até o presente momento foram para introduzir conceitos e mostrar em que situações um equipamento fabricado recentemente pode ser usado para introduzir melhorias em uma LAN corporativa: o switch que opera em camada 3 (camada de rede do modelo OSI), ou switch de camada 3.

Para delinear de que modo essas melhorias podem ser implementadas, é necessário adicionalmente explicar algumas funcionalidades que estão presentes em switches de camada 2 e camada 3, explicar a diferença entre eles e porque um switch de camada 3 pode ser mais eficiente que um switch de camada 2.

5.1 SWITCHES DE CAMADA 2

Como foi introduzido anteriormente, os switches são usados para conectar dispositivos de rede em encaminhar dados de uma porta a outra com base em informações obtidas a partir dos pacotes a serem transmitidos (LOWE, 2011).

Os switches de camada 2 aprendem os endereços MAC automaticamente, a construção de um tabela, a tabela de endereçamento MAC, que pode ser usada para transmitir seletivamente os pacotes. Por exemplo: se um switch recebe

dataframes a partir de um endereço MAC “X” através da porta 01, então sabe que os *dataframes* destinados ao endereço “X” podem simplesmente ser encaminhados através da porta 01, em vez de ter que tentar cada porta disponível, por sua vez (SOSINSKY, 2009).

Os switches de camada 2 podem ainda identificar e eliminar os *loops* (anéis) de dados (TECHGUIDE, 2013).

O que os switches de camada 2 não podem fazer é aplicar qualquer inteligência no encaminhamento dos pacotes. Eles não podem rotear pacotes com base no endereço IP ou priorizar pacotes enviados por aplicações específicas, como por exemplo, garantir a largura de banda para usuários de Voz sobre IP (VOIP). A informação necessária para tal só começa a tornar-se disponíveis na camada 3 (camada de rede).

5.2.1 Sub-redes (*subnets*)

Um *domínio de broadcast* é um espaço da rede lógica onde quadros de broadcast são enviados. Um *frame* de broadcast é um quadro de enlace de dados que é enviada a todos os dispositivos na rede e são tipicamente usados para localizar um dispositivo na rede (ANGELESCU, 2010).

As sub-redes são uma técnica que permite a criação de grupos de redes menores definidos logicamente. O propósito da criação das sub-redes é dividir uma grande LAN em pedaços lógicos menores e em domínios de *broadcast* menores (ANGELESCU, 2010).

Essa técnica permite aos administradores de rede utilizar os 32 bits disponíveis no endereçamento IP de modo mais eficiente, definindo que parte do endereçamento IP representa o ID de *host* e o ID de rede. Segundo a definição de classes de endereçamento IP existentes, há apenas 3 possibilidades existentes para se definir o

tamanho de ID de rede: 8, 16 e 24 bits. A técnica de criação de sub-redes permite a escolha arbitrária do número de bits para o uso do ID de rede (LOWE, 2011).

Para que as sub-redes funcionem, o roteador deve ser informado qual porção do host ID deve ser usada para se criar o novo ID de rede. Para tal, lança-se mão do uso de um número de 32 bits conhecido como máscara de sub-rede (LOWE, 2011).

Na prática, a LAN ficará dividida logicamente em LANs menores, sendo necessário uma conexão WAN no roteador para a conexão entre as sub-redes diferentes (LOWE, 2011).

5.2.2 Lans virtuais - VLANs

Um switch de camada 2 encaminha um frame de broadcast para toda a rede em todas as suas portas, exceto para a porta de onde o frame de broadcast entrou no switch. Isto pode tornar-se um problema em grandes redes e é aí que entra o uso das VLANs (ANGELESCU, 2010).

As sub-redes podem subdividir as LANs em porções menores de *hosts*. No entanto esta funcionalidade somente é possível quando os hosts se encontram dentro de uma mesma LAN física, ou seja, quando estão interconectados fisicamente. Uma funcionalidade amplamente usada e útil em uma LAN corporativa é a segmentação da LAN em sub-redes *lógicas*, ou virtuais: as VLANs, ou LANs virtuais. Por exemplo, os departamentos de engenharia e finanças de uma empresa podem ter computadores na mesma LAN física, porque eles estão na mesma ala do edifício, mas pode ser mais fácil de gerenciar o sistema se cada departamento tenha a sua própria rede, mesmo que elas fiquem separadas logicamente (SOSINSKY, 2009).

As VLANs estão descritas sob o padrão IEEE 802.1Q, que trata da padronização deste tipo de funcionalidade. Uma VLAN é um conjunto de hosts que são agrupados em um domínio de broadcast lógico que é independente de suas localizações físicas

(figura 18). O switch então encaminha pacotes de modo que computadores conectados às portas de uma determinada VLAN sejam separados dos computadores ligados às portas de outra VLAN. Os dados enviados a partir de um nó de uma rede para outro nó na rede aparecem como se uma rede remota fizesse parte da rede local. O tráfego de VLAN pode ser priorizado, agrupado e administrado a partir de uma console. Uma VLAN é uma definição de um agrupamento segregado em camada 2 e é utilizada para criar o equivalente de sub-redes em camada 3 de redes IP (EDWARDS e BRAMANTE, 2009).

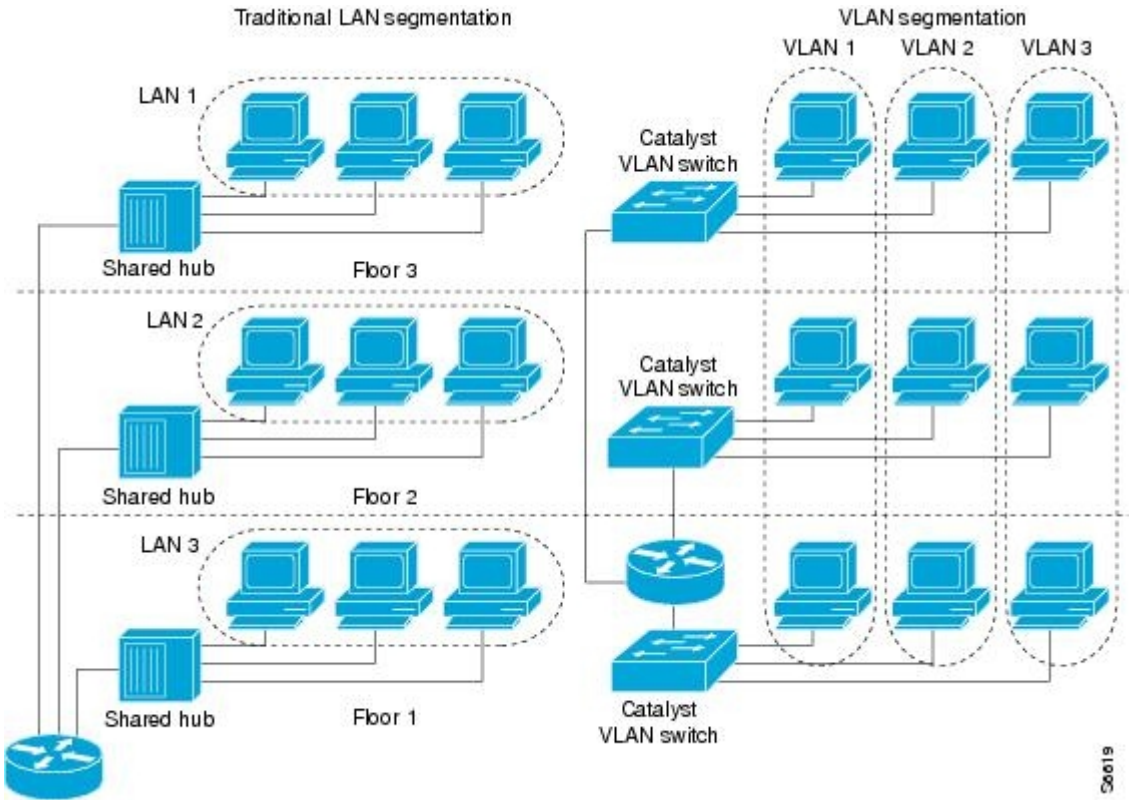

Figura 18 - segmentação de uma LAN em VLANs

Fonte: Cisco (2013)

Para oferecer suporte a recursos de VLAN, dois campos são inseridos no frame Ethernet: o campo ID do Tipo de VLAN, que identifica a estrutura como uma estrutura de VLAN; segundo campo é o campo *Control Information*, que contém um número de prioridade de 0 a 7 (mais alto) e a VLAN ID (identificador de grupo). Quando quadros Ethernet são marcados com campos VLAN, todos os nós participantes desta VLAN devem ter essa opção instalada (SOSINSKY, 2009).

As definições de VLAN são feitas a partir das configurações de portas do próprio switch e podem inclusive ser feitas entre 2 ou mais switches diferentes, ou seja, hosts conectados em portas de switches diferentes, e até de fabricantes diferentes, podem estar em uma mesma VLAN, como mostrado na figura 19, onde cada conjunto com cores iguais representa uma VLAN distinta. Notar que os switches podem estar fisicamente unidos, mas separados logicamente e vice-versa (TUHS, 2013).

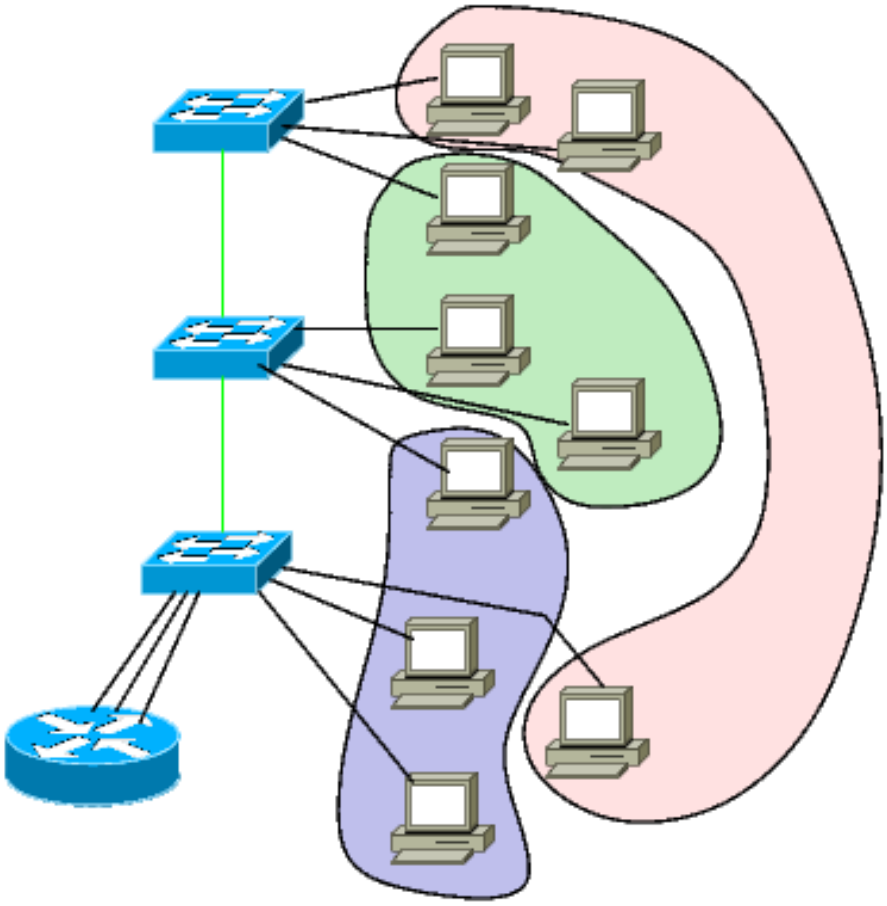

Figura 19 – VLANs criadas.

Fonte: Tuhs (2013)

Uma vez criadas as VLANs, o tráfego ficará isolado somente entre membros de uma mesma VLAN. Ou seja, mesmo que fisicamente unidos, os *hosts* de diferentes VLANs se comportam como LANs físicas separadas. Dessa forma o tráfego entre VLANs só pode ser roteado, como acontece na prática com tráfego entre LANs diferentes, e não mais encaminhado em camada 2 (ANGELESCU, 2010).

5.3 SWITCHES DE CAMADA 3

Switches de camada 2 podem encaminhar o tráfego com base em informações do *dataframe* da camada de enlace de dados, especificamente os endereços MAC (SOSINSKY, 2009).

Por outro lado, como visto anteriormente, um roteador é um dispositivo que liga duas redes diferentes. Os roteadores separam domínios de colisão, filtram e bloqueiam mensagens de broadcasts, e determinam o caminho ideal a ser usado para rotear pacotes. Como os roteadores operam na camada de rede (camada 3), os roteadores podem por vezes ser denominados switches de Camada 3, da mesma maneira que *bridges* podem ser referenciadas como switches de camada 2 (EDWARDS e BRAMANTE, 2009).

Os switches de camada 3, também chamados de switches de roteamento (do inglês *routing switch*), são capazes de encaminhar dados entre diferentes segmentos de rede. Tais switches usam uma combinação de protocolos de camada 2 com protocolos de camada 3, tendo assim a inteligência de roteadores com a flexibilidade de transmissão de dados utilizando protocolos de camada 2 (NORTEL NETWORKS, 2013). De acordo com Edwards e Bramante (2009), portanto, switches de camada 3 combinam as tecnologias de velocidade de cabeamento encontradas em switches de camada 2 e as ferramentas necessárias para rotear pacotes como um roteador convencional.

Assim, a diferença entre a comutação nas camadas 2 e 3 é o tipo de informação que há no interior da estrutura que é utilizada para determinar a interface de saída correta. Com a comutação em camada 2, os quadros são trocados com base nos endereços MAC. Com a comutação em camada 3, os quadros são trocados com base em informações da camada de rede, examinando as informações de pacotes e encaminhando-os com base em seus endereços de destino da camada de rede (TEILAM, 2013).

6 VANTAGENS DOS SWITCHES DE CAMADA 3 EM UMA LAN

6.1 ENCAMINHAMENTO DE TRÁFEGO A ALTAS VELOCIDADES

Os switches de camada 3 executam muitas das mesmas funções dos roteadores de modo muito mais rápido. Os roteadores convencionais dependem de software para implementar os protocolos de roteamento e as tomadas de decisão lógicas e utilizam um microprocessador para realizar a comutação de pacotes. Switches de camada 3 implementam o processo de decisão de roteamento exclusivamente em hardware, permitindo uma maior taxa de transferência de frames. Estes dispositivos de rede pode ser mais rápidos do que roteadores no encaminhamento de *dataframes*, mas eles não são tão flexíveis ou programáveis como um roteador convencional. Assim, eles oferecem o controle do fluxo de dados que é oferecido numa rede roteada e a velocidade que é oferecida num ambiente comutado (EDWARDS e BRAMANTE, 2009). A figura 20 mostra um exemplo de camada com a implantação de switches camada 3.

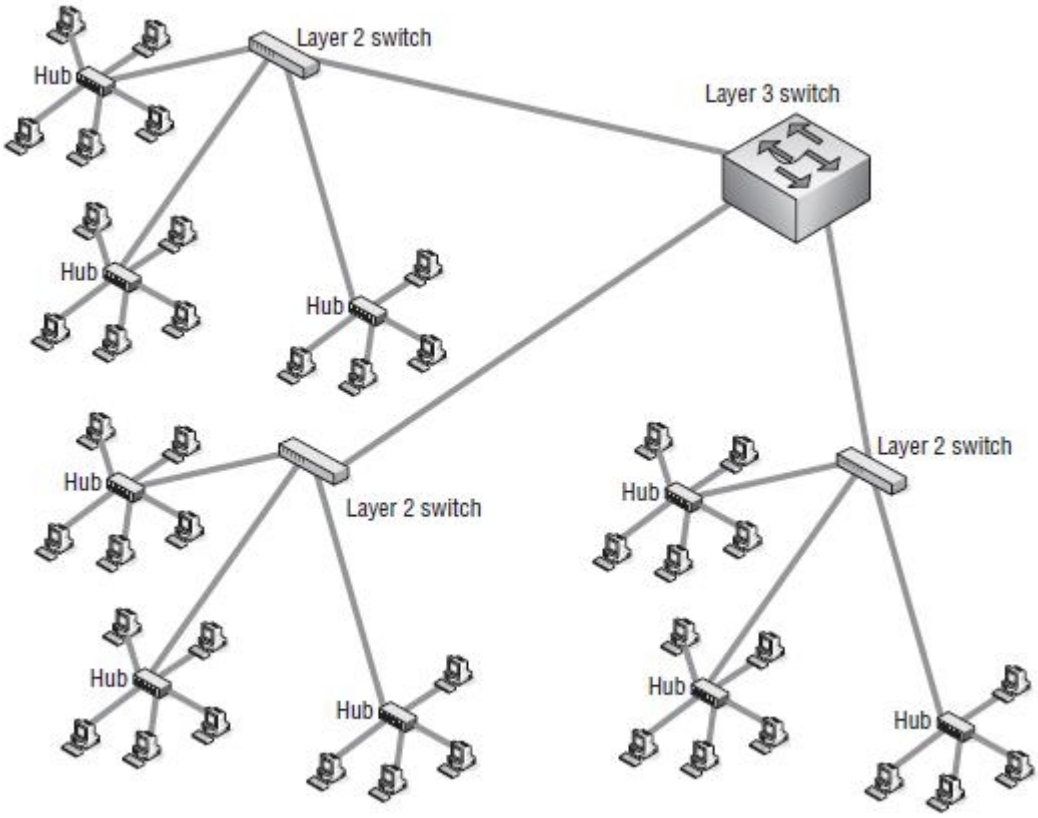

Figura 20 – Instalação de switches de camada 3 em uma LAN
Fonte: Edwards e Bramante (2009)

Switches de camada 3 tomam decisões de roteamento com base nas mesmas informações da tabela de roteamento de um roteador tradicional faz. Quanto ao design de hardware, um switch de camada 3 e um roteador são muito parecidos em muitos casos. Ambos são configuráveis e os equipamentos mais avançados possuem *slots* onde diferentes tipos de módulos podem ser inseridos, aumentando os protocolos que são suportados pelo equipamento (EDWARDS e BRAMANTE, 2009).

Os switches de camada 3 são predominantemente desenvolvido para LANs corporativas de maior abrangência. A Internet ainda utiliza roteadores no núcleo para obter dados para um destino. A maioria dos switches da Camada 3 não são capazes de suportar as interfaces WAN necessárias para o encaminhamento de dados da Internet, uma vez que switches são relacionados com o padrão Ethernet. Assim, os roteadores são usados ainda como fronteiras entre a LAN e a Internet. (EDWARDS e BRAMANTE, 2009).

Os roteadores ainda estão em uso hoje atualmente, porém os switches de camada 3 estão se tornando cada vez mais populares. A razão, segundo Edwards e Bramante (2009), é simples: os switches de camada 3 são capazes de atuar como um roteador em uma velocidade muito maior devido à tecnologia que implementa aplicações específicas em circuito integrado.

Na tabela 1 estão resumidas as diferenças e vantagens em termos de velocidade entre switches de camada 3 e roteadores (CHANG e HUANG, 2013):

Características	**Switch de camada 3**	**Roteador convencional**
Função principal	Comutação em camada 2 e roteamento em camada 3	Roteamento em camada 3
Arquitetura de encaminhamento de pacotes	ASIC (Application specific integrated circuit, ou circuito integrado de aplicação específica)	CPU + Software
Desempenho em encaminhamento de pacotes	ALTA (> 1Mpps)	BAIXA (< 1Mpps) - normalmente 500Kpps
Preço	Baixo	Alto

Tabela 1: diferenças entre switches de camada 3 e routers

Fonte: Chang e Huang (2013)

6.2 ROTEAMENTO ENTRE SUB-REDES E VLANS

Em certas situações, é necessário que mensagens que se originem a partir de um host de uma determinada sub-rede ou VLAN seja direcionado a uma outra sub-rede ou VLAN dentro da mesma LAN física. Essa necessidade não é suprida com os switches tradicionais, que somente podem encaminhar *dataframes* de camada 2

dentro da mesma sub-rede ou VLAN, uma vez ela criada dentro do switch. Deste modo, é necessário que um roteador localizado entre as 2 sub-redes ou VLANs faça o roteamento dos *dataframes*, como mostra a figura 21, com a conexão de um *host* em uma sub-rede 1 e um servidor em uma sub-rede 2 (HEWLLET & PACKARD, 2013).

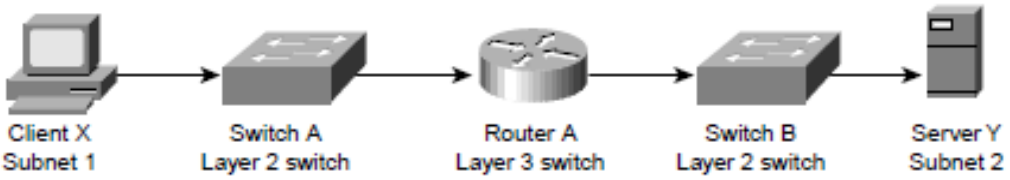

Figura 21 - Fluxo de tráfego entre sub-redes com switches de camada 2 e roteadores
Fonte: Teilam (2013)

A implementação do roteamento entre VLANs traz vantagens como (MENGA, 2013):

- A redução de domínios de *broadcast*, aumentando a performance e eficiência da rede;

- As topologias em múltiplas camadas baseadas em roteamente entre VLANs são muito mais escaláveis e implementam mecanismos eficientes para acomodar caminhos redundantes na rede que uma rede de camada 2 somente;

- Permite um controle de acesso de segurança centralizado entre cada uma das VLANs;

- Aumenta a facilidade de gerenciamento da rede isolando o efeito de um ponto de rede defeituoso a uma VLAN somente ao invés da rede toda.

Assim, ainda de acordo com Menga (2013), os benefícios de uma rede baseada em roteamento entre VLANs não pode prejudicar o desempenho da rede. Portanto, uma abordagem muito usada é a implementação de switches de camada 3.

Como os switches de camada 3 podem operar na camada 2, bem como funcionar como um roteador, eles podem ser configurados para tomar decisões de roteamento

para enviar dados a um destino. Assim, switches de camada 3 podem rotear o tráfego com base em informações de camada de rede e encaminhar pacotes entre diferentes VLANs. Ademais, um switch camada 3 possui uma latência, ou seja, o tempo de resposta a uma solicitação, bem mais baixa que um roteador (ANGELESCU, 2010).

Para rotear o tráfego, os switches de camada 3 devem ter a rota IP apropriada. Assim, eles suportam rotas estáticas configuráveis e rotas aprendidas através de um protocolo. Alguns switches suportam apenas rotas estáticas e às vezes são chamados de "*light layer 3 switches*", ou switches de camada 3. Desse modo, switches de camada 3 têm substituído a necessidade de decisões lógicas de software dos roteadores e contam com circuitos integrados para executar essas tarefas (HEWLLET & PACKARD, 2013). A figura 22 mostra como é feita a substituição de um roteador por switch de camada 3.

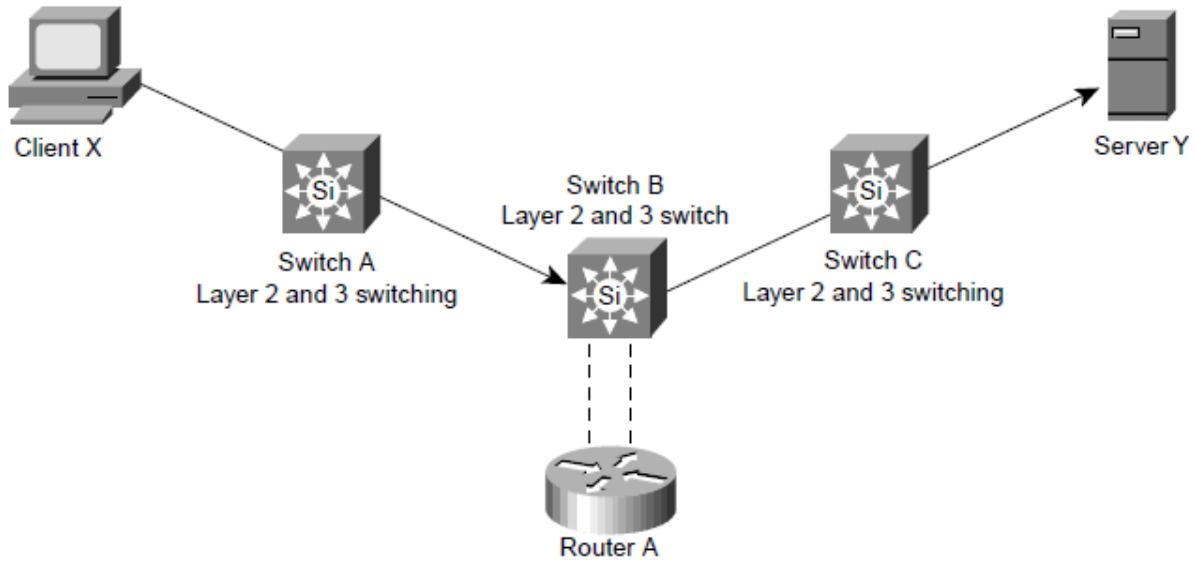

Figura 22 - Fluxo de tráfego entre sub-redes com switches de camada 3

Fonte: Teilam (2013)

Como definido anteriormente, a função de roteamento é importante quando um host em uma rede precisa enviar um pacote para um computador em outra rede (LAN ou VLAN). Para esta tarefa é necessário o uso de um roteador para encaminhar o pacote para a rede de destino. Em alguns casos, um pacote pode, na verdade, ter

que viajar através de várias redes intermediárias, sendo roteado diversas vezes a fim de atingir o seu destino de rede final (TANENBAUM, 2011).

Uma das grandes vantagens de um switch de camada 3 é a possibilidade de fazer o tráfego fluir entre 2 ou mais VLANs distintas. Se o host de origem e o de destino não estiverem dentro de uma mesma sub-rede ou VLAN, os pacotes irão ser encaminhados baseados na informação de endereço IP da camada 3 do modelo OSI (ANGELESCU, 2010).

Esta camada, além das características já mencionadas, fornece particionamento lógico de sub-redes, escalabilidade, segurança e a implementação de políticas de QoS (explicado adiante), um recente incremento das funcionalidades de camada 3, que vai além da priorização de pacotes simples encontrados em CoS (Class of Service), proporcionando reserva de banda e atraso de pacotes, se necessário. Os switches de camada 3 possuem a capacidade de identificar qual é o tipo de pacote que está sendo originado e, se houver a necessidade de encaminhá-lo para um host externo à VLAN ou a sub-rede, o switch tem a capacidade de rotear o pacote. O processo de encaminhamento em camada 3 consiste em ler o endereço IP de destino e então consultar a tabela de roteamento interna do switch para determinar o endereço do próximo salto da rede baseado em seu endereço MAC (3COM, 2013).

Neste sentido, em uma rede LAN com muitos hosts essa é uma grande vantagem, pois um roteador é normalmente ligado a uma das portas do switch e efetua o papel de rotear os pacotes entre VLANs. Este roteador é muitas vezes referido como um roteador “maneta”, uma vez que recebe e transmite o tráfego sobre a mesma port. Na realidade, tais roteadores se conectam a outros switches ou redes de longa distância (WANs). Os switches de camada 3 oferecem a funcionalidade de roteamento dentro da mesma caixa, evitando um uso de um roteador e, assim, liberam outra porta do switch (SRIDHAR, 1998).

Switches de camada 3 switches podem funcionar como roteadores tradicionais conectando vários switches Layer 2 e fornecer conectividade inter-VLAN. Em tais casos, não existe nenhuma funcionalidade deste tipo em switches de Camada 2. Este conceito pode ser ilustrado pela colocação de um switch de camada 3 puro

entre a camada de um switch de camada 2 e o roteador (CHANG e HUANG, 2013). O Switch Layer 3 aliviaria o roteador do processamento inter-VLAN. A figura 23 ilustra esse caso:

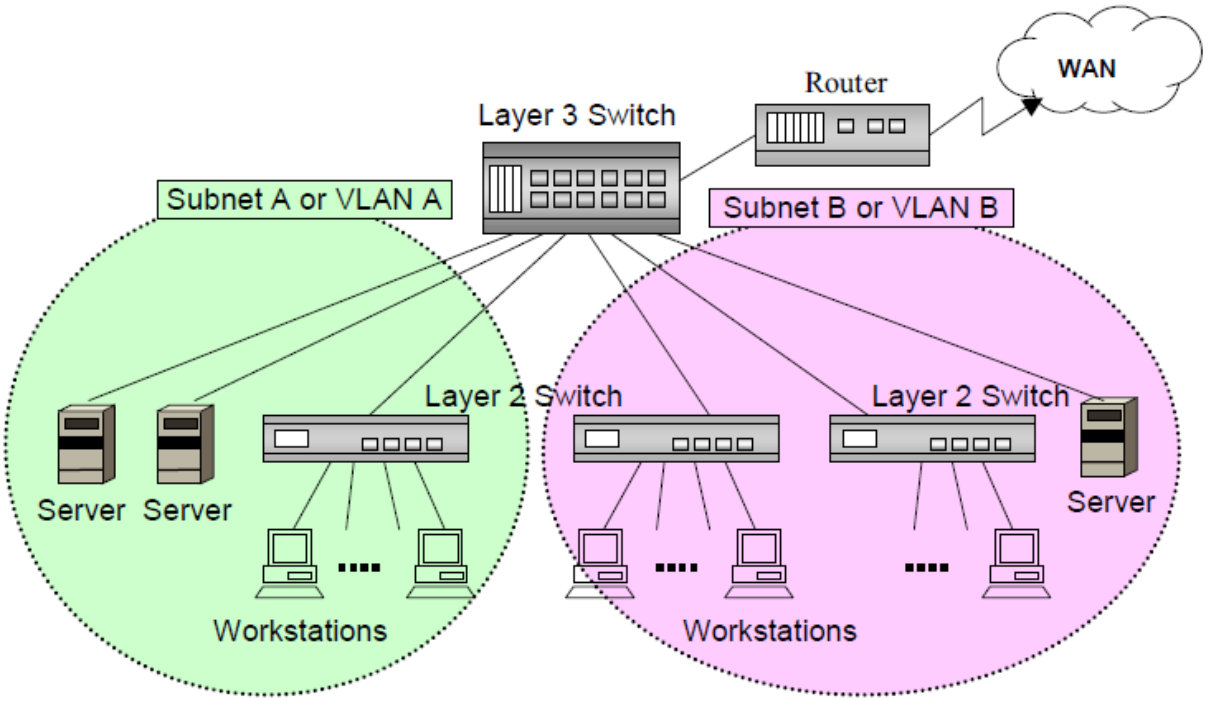

Figura 23 – Uso de um switch de camada 3 para melhorar o desempenho da rede

Fonte: Chang e Huang (2013)

Além das funcionalidades de roteamento, switches layer 3 empregam balanceamento de carga e podem distribuir o tráfego sobre todas as suas portas de rede que possuem a mesma distância a partir do endereço de destino. O balanceamento de carga aumenta a utilização de segmentos de rede, aumentando assim a largura de banda efetiva. A comutação em camada 3 efetua o balanceamento de carga baseado no destino e origem dos pacote IP (3COM, 2013).

De acordo com a 3COM (2013), os roteadores tradicionais, uma vez que são componentes fundamentais de redes corporativas, tornaram-se um grande obstáculo à migração para redes de próxima geração. Porém é interessante notar que um switch camada 3 faz de tudo para um pacote que um roteador tradicional faz:

• Determina o caminho do encaminhamento com base nas informações da camada 3;

• Valida a integridade da camada 3 por meio da soma de verificação do dataframe;
• Verifica a validade de pacotes e efetua atualizações sobre eles;
• Processa e responde a todas as informações da opção;
• Efetua atualizações estatísticas encaminhamento do protocolo Management Information Base (MIB);
• Aplica controles de segurança, se necessário.

6.3 DIFERENCIAÇÃO E PRIORIZAÇÃO DE TRÁFEGO (QoS)

Switches de camada 3 também têm a capacidade de controlar o fluxo de dados, implementando o que é conhecido como a qualidade de serviço (QoS), que prevê o enfileiramento de pacotes em classes de serviço para garantir que dados com maior prioridade sejam atendidos antes de outros dados com menor prioridade (3COM, 2013).

A aplicação de políticas é um mecanismo para alterar o encaminhamento normal de um pacote através de um dispositivo de rede. Exemplos incluem segurança e balanceamento de carga. Políticas mais recentes incluem QoS, uma maneira de alocar largura de banda e controle de propagação atrasar, de forma a gerir priorização de pacote. As políticas de QoS não apenas significam a aplicação de novas aplicações multimídia, como telefonia LAN, mas para garantir o tempo de resposta da rede para aplicações de missão crítica, como a telemedicina (3COM, 2013).

Chamado o padrão 802.1p, este protocolo permite que dispositivos apliquem a qualidade de serviço (QoS) para identificar e priorizar certos tipo de tráfego. Este tipo de funcionalidade permite que certas aplicações sensíveis a atrasos (tais como voz sobre IP, ou VoIP) recebam tratamento prioritário (3COM, 2013).

A classe a que os pacotes pertencem determinam a programação de pacotes e políticas de descarte. Por exemplo, o serviço geral dada aos pacotes na classe

premium vai ser melhor do que o indicado para a classe padrão, a classe premium está prevista para experimentar a menor taxa de perda ou atraso (3COM, 2013).

O switch de camada 3 tem encaminhamento baseado em QoS para o tráfego IP. A implementação de encaminhamento QoS é baseada em política administrativa local e precedência do endereço IP. O mapeamento entre os campos de precedência de IP e os campos de QoS de atraso determina a prioridade do pacote (3COM, 2013).

6.4 APRENDIZADO DE ROTAS (PROTOCOLOS RIP E OSPF)

As rotas em camada 3 são aprendidas estática ou dinamicamente. As estáticas são configuradas manualmente, pelo administrador da rede. As rotas dinâmicas são aprendidas e construídas pelos roteadores e switches de camada 3 (HEWLLET & PACKARD, 2013).

Como é projetado para lidar com o tráfego LAN de alta performance, um switch de camada 3 pode ser colocado em qualquer lugar dentro de um core de rede ou backbone, de forma fácil e econômica substituindo o roteador de backbone tradicional. O switch camada 3 se comunica com o roteador WAN usando protocolos de roteamento padrão da indústria, como RIP e OSPF (HEWLLET & PACKARD, 2013).

Os protocolos de roteamento *Open Shortest Path First* (OSPF) e *Routing Information Protocol* (RIP) fornecem informações para dispositivos de camada 3 para o tráfego de dados direto para o destino pretendido. Em resumo, os switches de camada 3 podem ser entendidos como roteadores com roteamento rápido feito via hardware. O encaminhamento IP geralmente envolve uma pesquisa de rota e encaminhamento do dataframe com o endereço MAC apropriado no cabeçalho para a porta de saída correta. Os roteadores executam os protocolos de roteamento como o OSPF ou o RIP para se comunicar com outros switches de camada 3 ou roteadores e criar suas

tabelas de roteamento. Estas tabelas de roteamento são pesquisadas para determinar a rota para um pacote de entrada (SRIDHAR, 1998).

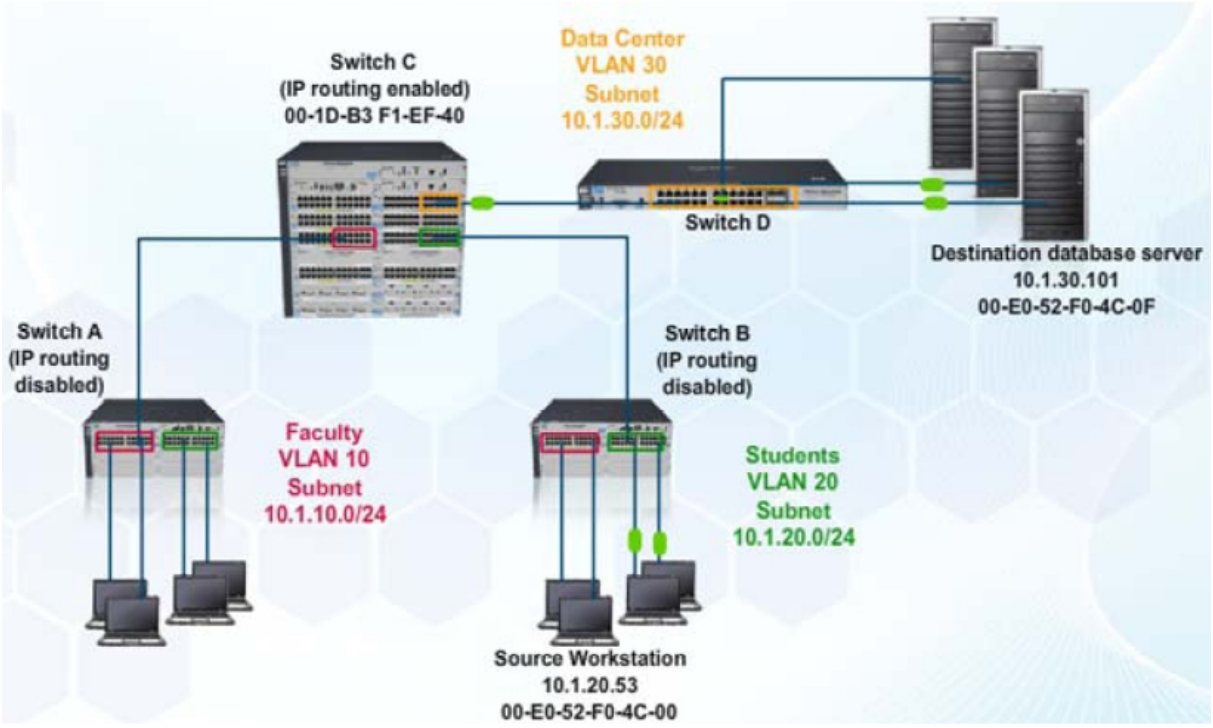

Figura 24 – Exemplo de roteamento

Fonte: Hewllet & Packard (2013)

Abaixo um exemplo fornecido por Hewllet & Packard (2013), de como é feito um roteamento com switches layer 3. A figura 24 mostra um exemplo de uma estação (*host*) de um estudante na VLAN 20, denominada de *students* que quer acessar um servidor em um *datacenter*. Para acessar esse servidor a estação do estudante endereça um pacote IP ao servidor *database*. Assim, a estação do estudante deve então encapsular o pacote IP em um *dataframe* de Ethernet e para tal deve incluir no cabeçalho do *dataframe* o endereço MAC de destino. Como a estação não tem como saber o endereço MAC do servidor *database*, e que e ele se localiza na VLAN 30 (diferente da VLAN *students*) então ela fornece o endereço MAC de seu *gateway*, o switch C, como o endereço MAC destino ao cabeçalho Ethernet. Portanto, o cabeçalho do dataframe Ethernet conterá o endereço do *gateway* (que neste exemplo é 00-1D-B3-F1-EF-40) e o endereço IP do servidor *database* (neste caso, 10.1.30.101).

A estação do estudante envia então um *dataframe* Ethernet para o switch que está diretamente conectado a ela (switch B), que não possui a função de roteamento habilitado. O switch B procura em sua tabela de encaminhamento (tabela 2) o endereço MAC destino fornecido pela estação. Como o endereço MAC fornecido é do switch C, que possui o endereço IP 10.1.10.1, então o switch B encaminha o *dataframe* para o switch C através da porta física B17.

IP Address	MAC Address	Type Port
10.1.20.15	001aa0-1f8deb	dynamic B15
10.1.20.1	001db3-f1ef40	dynamic B17
10.1.20.101	001ec3-10e80b	dynamic B19
10.1.10.34	001ac9-f5d4bf	dynamic A10
10.1.10.1	001db3-f1ef40	dynamic B17

Tabela 2 – Tabela de encaminhamento do switch B

Fonte: Hewllet & Packard (2013)

O switch C, por sua vez, analisa o *dataframe* e reconhece o endereço MAC fornecido como seu próprio endereço. Assim, ele determina que deve usar a informação de camada 3 (endereço IP) para tomar uma decisão de encaminhamento. Assim, ele elimina o cabeçalho Ethernet e passa a usar a sua tabela de roteamento para encontrar um correspondente para o pacote IP fornecido (Tabela 3).

Destination	Gateway	VLAN	Type	Sub-Type	Metric	Dist
10.1.2.0/24	DEFAULT_VLAN	1	connected		1	0
10.1.10.0/24	VLAN10	10	connected		1	0
10.1.20.0/24	VLAN20	20	connected		1	0
10.1.30./24	VLAN30	30	connected		1	0
127.0.0.0/8	Reject		static		0	0
127.0.0.1/32	lo0		connected		1	0

Tabela 3 – Tabela de roteamento do switch C

Fonte: Hewllet & Packard (2013)

Como a tabela 3 mostra, o swtich possui uma rota direta, ou seja, diretamente conectada a ele, para o endereço IP 10.1.30.0. Então o switch C verifica sua tabela de encaminhamento se ele possui registro contendo o endereço MAC corresponde ao endereço IP 10.1.30.0. Se não houver, então ele envia uma requisição ARP (de *Address Resolution Protocol*), que é uma mensagem de *broadcast* que solicita aos hosts o envio do endereço IP correspondente. Finalmente, o switch C cria um novo cabeçalho Ethernet para o pacote IP, usando o endereço MAC do servidor *database*. O switch D então recebe o *dataframe*, verifica a sua tabela de encaminhamento e encaminha o tráfego para a porta correspondente à do servidor *database*.

Como conclusão, ~~podemos~~ pode-se ver que o switch de camada 3 não elimina a necessidade de se ter um roteador na rede, especialmente porque os roteadores ainda são necessários para se conectar a rede à Internet (via interface WAN). Assim, os switches de camada 3 têm a sua funcionalidade efetivada no *backbone* (camada *core*) de uma rede, mas não nas bordas (camada de acesso) de conexão com uma WAN (SRIDHAR, 1998).

7 CONCLUSÃO

O objetivo deste trabalho foi o de evidenciar como os switches de camada 3 se inserem nas redes de computadores corporativas e de que modo eles podem contribuir com a melhoria do desempenho das redes.

Entre as saídas para melhorar o tráfego em redes locais corporativas estão o incremento com maior número ou equipamentos mais velozes. Ou então a adição de equipamentos que possam processar o tráfego que flui pelas redes de modo mais eficiente e inteligente. Essa foi a proposta deste trabalho.

Conclui-se que a adição de switches de camada 3 em redes locais melhora o desempenho global da rede quando se trata de redes com maior número de hosts. O custo de equipamentos que efetuam roteamento e encaminhamento existe desde os anos 1990 e desde então decresce gradativamente e passa a tornar os switches de camada 3 cada vez mais presentes em redes locais.

A grande vantagem desse tipo de equipamento é sua estrutura de fabricação, uma vez que diferentemente de roteadores, que implementam o roteamento em software, os switches de camada 3 possuem essa funcionalidade implementadas diretamente no hardware. Desse modo, tais switches são de extrema importância para encaminhar, principalmente, o tráfego inter-VLAN, que só pode ser feito em camada 3.

Quer parecer que a tendência é uma fusão entre os switches layer 3 e roteadores, de modo a se criar equipamentos híbridos. No entanto, em vista da necessidade de conexão com a Internet, os roteadores possuem sua função e utilidade garantidas. O estado da arte atualmente reside no uso simultâneo e o aproveitamento de ambas funcionalidades dos equipamentos.

8 REFERÊNCIAS BIBLIOGRÁFICAS

3COM. **Layer 3 Switching - An Introduction.** Disponível em: <http://www.zwaga.com/info/net/netwerk/pdf/Layer3Switching.pdf> Acesso em: 29 de Agosto de 2013

ANGELESCU, Silviu. **CCNA Certification All-in-one for dummies**. 1.Ed. Indianapolis: Wiley, 2010

CHANG, George; HUANG, Minju. **Introduction to Layer 2/3 Switches**. Disponível em: <ftp://ftp.dlink.es/Switch/Miscellaneous/Manuali%20Tecnici%20comuni%20PDF/Switch-Layer3_1-8-01.pdf> Acesso em: 29 de Agosto de 2013

CISCO. **Routing Between VLANs Overview.** Disponível em: <http://www.cisco.com/en/US/docs/ios/12_2/switch/configuration/guide/xcfvl.pdf>. Acesso em: 27 de Agosto de 2013

DLINK. **Business Solution.** Disponível em: <http://www.dlink.com/es/es/business-solutions/switching/smart-switches/smart/dgs-1210-series-gigabit-smart-switches>. Acesso em: 30 de Agosto de 2013.

EDWARDS, James; BRAMANTE, Richard. **Networking - Self Teaching Guide**. 1.Ed. Indianapolis: Wiley, 2009

HEWLLET & PACKARD. **Getting Started with HP Switching and Routing.** Version 10.41. Disponível em: <ftp://ftp.lanit.ru/Technical/HPN_doc/Getting_Started_Switching_and_Routing_v10.41-Letter.pdf>. Acesso em: 25 de Agosto de 2013

HINETWORLD. **Network topology.** Disponível em: <http://hinetworld.wordpress.com/2012/11/22/network-topology/> Acesso em: 29 de Agosto de 2013

IFSC. **Redes de Computadores II**. Disponível em <http://wiki.sj.ifsc.edu.br/wiki/index.php/RCO2-2012-2> Acesso em: 28 de Agosto de 2013

ITPRO. **Layer 2 and Layer 3 switches**. Disponível em <http://www.itpro.co.uk/88699/layer-2-and-layer-3-switches> Acesso em: 27 de Agosto de 2013

LOWE, Doug. **Networking All-in-one for dummies**. 4.ed. Indianapolis: Wiley, 2011

MENGA, Justin. **CCNP Practical Studies: Layer 3 Switching**. Disponível em: < http://www.ciscopress.com/articles/article.asp?p=102093>. Acesso em: 27 de Agosto de 2013

NORTEL NETWORKS. **Network Switching Technology - Layer 3 Switches**. Disponível em: <http://k-12.pisd.edu/currinst/network/08_805A_2-3_SG.pdf> Acesso em: 30 de Agosto de 2013

PRATICALLY NETWORKED. **Port Expand.** Disponível em: <http://www.practicallynetworked.com/networking/port_expand.htm> Acesso em: 30 de Agosto de 2013

RYAN, Jerry. **Overview of Layer 3 Switching and Software Features.** Disponível em: http://www.cisco.com/en/US/docs/switches/lan/catalyst2948gand4908g/12.0_7_w5_15d/configuration/guide/overview.pdf. Acesso em: 27 de Agosto de 2013

SRIDHAR, Thayumanavan. **Layer 2 and Layer 3 Switch Evolution**. The Internet Protocol Journal, V.51, n.3, p. 38-43. Mai/Jun. 1998. Disponível em <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-2/ipj_1-2.pdf>. Acesso em: 26 de Agosto de 2013

SOSINSKY, Barrie. **Networking Bible**. 1.ed. Indianápolis: Wiley, 2009

TANENBAUM, A. S. **Computer Networks**. 5.ed. Boston: Prentice Hall, 2011

TECHGUIDE. **Layer 3 Switching - Re-Inventing the Router.** Disponível em: <http://www.scom.uminho.pt/uploads/Apoio%20-%20Doc%20Tec%20-%203switch.pdf> Acesso em: 27 de Agosto de 2013

TEILAM. **Internetworking Design Basics.** Disponível em: <http://users.teilam.gr/~skontos/tei_site/html/pdf_cisco/internetwork_Design_Basic.pdf> Acesso em: 26 de Agosto de 2013

TUHS. **Networks and Applications - Switches, LAN Design, VLANs.** Disponível em: <http://minnie.tuhs.org/NC1/Lectures/lect03.html> Acesso em: 26 de Agosto de 2013

WEBPRONEWS. **Understanding Network Models** – The Cisco Network Design Model. Disponível em: <http://www.webpronews.com/understanding-network-models-the-cisco-network-design-model-2004-02> Acesso em: 29 de Agosto de 2013